PCT/JP03/10378

# 日本国特許庁
# JAPAN PATENT OFFICE

15.08.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.



出願年月日
Date of Application: ２００２年　８月２８日

出願番号
Application Number: 特願２００２－２４８８１２

[ST. 10/C]: [ＪＰ２００２－２４８８１２]

出願人
Applicant(s): 日本放送協会



２００３年　９月１９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　2002-123
【提出日】　平成14年 8月28日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都世田谷区砧一丁目１０番１１号
　日本放送協会　放送技術研究所内
　【氏名】　西本　友成
【発明者】
　【住所又は居所】　東京都世田谷区砧一丁目１０番１１号
　日本放送協会　放送技術研究所内
　【氏名】　栗岡　辰弥
【発明者】
　【住所又は居所】　東京都世田谷区砧一丁目１０番１１号
　日本放送協会　放送技術研究所内
　【氏名】　難波　誠一
【特許出願人】
　【識別番号】　000004352
　【氏名又は名称】　日本放送協会
【代理人】
　【識別番号】　100064414
　【弁理士】
　【氏名又は名称】　磯野　道造
　【電話番号】　03-5211-2488
【手数料の表示】
　【予納台帳番号】　015392
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0015226

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラム

【特許請求の範囲】

【請求項１】　受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行うコンテンツ送信方法であって、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理ステップと、

前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間情報を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、

前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化ステップと、

前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力ステップと、

を含むことを特徴とするコンテンツ送信方法。

【請求項２】　受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行うコンテンツ送信装置であって、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、

前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテン

ツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理手段と、

前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、

前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化手段と、

前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力手段と、

を備えることを特徴とするコンテンツ送信装置。

【請求項３】　前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間に対応する値として関連付けることを特徴とする請求項２に記載のコンテンツ送信装置。

【請求項４】　前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間とは異なる不均一な値として関連付けることを特徴とする請求項２に記載のコンテンツ送信装置。

【請求項５】　前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間に対して増減した値として関連付けることを特徴とする請求項２に記載のコンテンツ送信装置。

【請求項６】　前記コンテンツの先頭に、予め、当該コンテンツの任意部分を取り出した試視聴用のプレビュー用コンテンツを配置し、このプレビュー用コンテンツを前記第二暗号化鍵で暗号化するプレビュー用コンテンツ付加手段を備えたことを特徴とする請求項２から請求項５のいずれか１項に記載のコンテンツ送信装置。

【請求項７】　前記コンテンツを受信側で購入または借用された場合に料金を徴収する有料コンテンツである場合、前記受信側で当該有料コンテンツを購入または借用したかどうかを判定する購入フラグを前記コンテンツ利用制御情報内に設定する購入フラグ設定手段を備え、

前記有料コンテンツが前記受信側で購入または借用された場合に受信側から返

信される購入フラグに基づいて、前記有料コンテンツの徴収料金を確認する有料コンテンツ徴収料金確認手段を備えたことを特徴とする請求項２から請求項６のいずれか１項に記載のコンテンツ送信装置。

【請求項８】　前記多重出力手段が、前記第二暗号鍵関連情報を、前記暗号化コンテンツおよび前記第一暗号鍵関連情報に多重化せずに、前記受信側からの要求に基づいて前記第二暗号鍵関連情報を出力することを特徴とする請求項２から請求項７のいずれか１項に記載のコンテンツ送信装置。

【請求項９】　受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行う装置を、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段、

前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理手段、

前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化手段、

前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化手段、

前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力手段、

として機能させることを特徴とするコンテンツ送信プログラム。

【請求項１０】　請求項１記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にするコンテンツ受信方法であって、

前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離ステップと、

この受信分離ステップにて分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄積装置に蓄積する暗号化コンテンツ蓄積ステップと、

前記第二暗号鍵関連情報を、送信側に備えられている第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得ステップと、

前記蓄積装置に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得ステップにて取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得ステップと、

前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定ステップと、

この視聴可能判定ステップにおける判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力ステップと、

を含むことを特徴とするコンテンツ受信方法。

【請求項１１】　請求項２記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にするコンテンツ受信装置であって、

前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離手段と、

この受信分離手段で分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄

積する暗号化コンテンツ蓄積手段と、

前記第二暗号鍵関連情報を、送信側に備えられている第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得手段と、

前記暗号化コンテンツ蓄積手段に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得手段で取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得手段と、

前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定手段と、

この視聴可能判定手段における判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力手段と、

を備えることを特徴とするコンテンツ受信装置。

【請求項１２】　前記暗号化コンテンツを前記第一暗号鍵で復号化して再生した再生時間をカウントする再生時間カウント手段と、

前記コンテンツ利用制御情報に設定されている購入フラグを管理し、当該購入フラグにより前記暗号化コンテンツが有料である場合、前記再生時間カウント手段によってカウントした再生時間に応じて課金する課金手段とを備え、

前記視聴可能判定手段は、前記再生時間と、前記コンテンツ利用制御情報に含まれる予め指定された再生許可時間とを比較判定し、この比較判定に基づき、前記課金手段は、前記再生時間が前記再生許可時間を経過するまで課金しないことを特徴とする請求項１１に記載のコンテンツ受信装置。

【請求項１３】　前記再生時間カウント手段は、前記暗号化コンテンツの特定部分を異なる視聴形態でノンリニア再生した再生時間を、前記第一暗号鍵関連情報に含まれている前記第一暗号鍵が変更される変更単位時間に対応して付される連続指標に基づいて、カウントすることを特徴とする請求項１２に記載のコン

テンツ受信装置。

【請求項１４】　記憶した情報が外部より読みとり不可能なセキュリティモジュールを備え、

前記視聴可能判定手段による前記再生時間と前記再生許可時間との比較判定を、前記セキュリティモジュールの内部で行うことを特徴とする請求項１２または請求項１３に記載のコンテンツ受信装置。

【請求項１５】　前記セキュリティモジュールの内部で、前記第二暗号鍵関連情報を扱う場合、前記課金手段で、前記暗号化コンテンツを識別する識別子であるコンテンツＩＤ毎に、前記第二暗号鍵関連情報に含まれているコンテンツ利用制御情報を関連付け、前記再生時間カウント手段でカウントした再生時間を、前記コンテンツ利用制御情報に含めたコンテンツ履歴情報とすることを特徴とする請求項１４に記載のコンテンツ受信装置。

【請求項１６】　前記視聴可能判定手段で前記再生時間と前記再生許可時間との比較判定した判定結果、前記再生時間が前記再生許可時間に達していない場合、前記コンテンツ履歴情報および前記第二暗号鍵を含む関連情報を前記セキュリティモジュールの内部に備えられる固有鍵で再暗号化した再暗号化第二暗号鍵関連情報とし、この再暗号化第二暗号鍵関連情報を前記暗号化コンテンツ蓄積手段に記憶させる再暗号化手段を備えることを特徴とする請求項１５に記載のコンテンツ受信装置。

【請求項１７】　前記第二暗号鍵関連情報を前記暗号化コンテンツと共に、前記暗号化コンテンツ蓄積手段に蓄積する場合、前記再暗号化手段で再暗号化して前記暗号化コンテンツ蓄積手段に記憶させることを特徴とする請求項１６に記載のコンテンツ受信装置。

【請求項１８】　前記課金手段は、前記有料コンテンツを購入するか借用するかに関する情報を、通信回線網を介して、前記コンテンツ送信装置に通知することを特徴とする請求項１２から請求項１７のいずれか１項に記載のコンテンツ受信装置。

【請求項１９】　前記多重暗号化コンテンツに前記第二暗号鍵関連情報が多重化されていない場合、前記第二暗号鍵関連情報を、通信回線網を介して前記コ

ンテンツ送信装置に要求する第二暗号鍵関連情報要求手段を備え、

前記暗号化コンテンツが有料コンテンツである場合、前記課金手段が、前記第二暗号鍵関連情報を取得する際に、前記有料コンテンツにかかる料金を課金することを特徴とする請求項１２から請求項１８のいずれか１項に記載のコンテンツ受信装置。

【請求項２０】　請求項９記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする装置を、

前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離手段、

この受信分離手段で分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄積する暗号化コンテンツ蓄積手段、

前記第二暗号鍵関連情報を、送信側に備えられている第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得手段、

前記暗号化コンテンツ蓄積手段に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得手段で取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得手段、

前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定手段、

この視聴可能判定手段における判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力手段、

として機能させることを特徴とするコンテンツ受信プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、受信側で蓄積したコンテンツの任意部分をプレビューし、課金するコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムに関する。

【０００２】

【従来の技術】

従来、放送局等のコンテンツ送信側（コンテンツ提供側）から送信されたコンテンツ（番組等）が有料である場合、つまり、有料放送によって有料コンテンツ（通常、スクランブルされているコンテンツ）が視聴者に提供される場合、当該有料コンテンツを視聴した視聴者に対し、課金する方式として、実際にコンテンツを視聴した場合にのみ課金されるペイパービュー方式と呼ばれるものがある。

【０００３】

このペイパービュー方式は、視聴者が何らかの方法で、当該有料コンテンツの内容（スクランブルされているコンテンツの一部がデスクランブルされたもの）を確認してから、有料コンテンツを視聴することで課金されることを承諾する決定操作（視聴者が所持しているコンテンツ受信装置の決定操作：コンテンツ受信側）に基づいて課金が行われる方式である。

【０００４】

また、ここで述べた、有料コンテンツの内容を確認する何らかの方法の一つにプレビュー方式と呼ばれる方式があり、このプレビュー方式は、一般的に、定められた期間（例えば、コンテンツが配布されてから数ヶ月）内で、コンテンツの開始から限度内の時間では、コンテンツ送信側（コンテンツ提供側）でスクランブルされたコンテンツの一部がデスクランブル可能に構成されており、このデスクランブルされたコンテンツの一部を視聴者が視聴しても課金されない方式である。なお、このプレビュー方式の運用形態の例は、電波産業会（ＡＲＩＢ）の標準規格「デジタル放送における限定受信方式」（ＡＲＩＢ　ＳＴＤ－Ｂ２５）第

３．０版の第１部参考１の７「ＰＰＶ番組プレビュー機能の運用事例」に記載されている。

【０００５】

ところで、現在のところ、放送局等のコンテンツ送信側から送信されるコンテンツがデジタルである場合、つまり、デジタル放送であり、さらにＰＰＶ放送（ペイパービュー放送）が行われる場合、コンテンツをスクランブルするスクランブル鍵Ｋｓを配布するＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）内に現在時刻およびプレビューを許可する時間情報が設定されており、デジタルコンテンツ（以下、デジタルコンテンツも「コンテンツ」に表現を統一する）のプレビューが実現されている（プレビュー機能が提供されている）。

【０００６】

【発明が解決しようとする課題】

しかしながら、従来のプレビュー機能は、コンテンツをリアルタイムに視聴する場合を想定したものであり、受信側の視聴者の視聴形態の多様化に伴い、コンテンツをリアルタイムに視聴する際の通常の視聴形態（リアルタイムにプレビューを見た後でコンテンツを購入する）とは異なったコンテンツの視聴形態の実現が望まれている。すなわち、コンテンツを一旦蓄積した後、受信側の視聴者が都合のいい時間に、コンテンツの一部をプレビューし、このプレビューを視聴した後に気に入れば購入するといった視聴形態、つまり、限定受信方式に則したプレビュー方式の実現が要望されている。

【０００７】

例えば、従来のプレビュー機能は、コンテンツをリアルタイムに視聴する場合のみが想定されており、現在時刻に基づいて、コンテンツをプレビューする許可が決定（プレビュー判定）されていたので、当該コンテンツを蓄積した後、再生する蓄積再生時に生じうる、コンテンツのノンリニア再生、巻き戻し操作等に対応させたプレビュー判定が行うことができないという問題がある。つまり、蓄積再生時におけるプレビューができないという問題がある。

【０００８】

また、従来のプレビュー機能は、放送局等のコンテンツ送信側から送信されたコンテンツを受信した際のプレビュー機能であったので、従来のプレビュー機能では、コンテンツ受信側で当該コンテンツを再生する場合に、専用に編集または制作したプレビュー用コンテンツを取り扱うことができないという問題がある。

【０００９】

或いは、従来のプレビュー機能は、蓄積再生時におけるプレビューが想定されておらず、蓄積されたコンテンツのプレビューの再生時間を制御することができないという問題がある。

【００１０】

換言すれば、従来のプレビュー機能は、リアルタイムに放送されるコンテンツを、コンテンツ受信側で受信して視聴する「限定受信方式」を想定したものであり、放送されたコンテンツの信号がスクランブルされた状態で蓄積装置等に蓄積され、再生時にデスクランブルされて視聴される、いわゆるホームサーバ等の蓄積受信システムにおける「限定再生」を想定したものではない。

【００１１】

つまり、従来のプレビュー機能は、リアルタイム時用のプレビューに対応したものであり、プレビューを視聴後、コンテンツを蓄積する場合は、当該コンテンツを購入（コンテンツ購入確認後）してからでないとできない。なぜならば、コンテンツ受信側で「限定再生」を実行する場合には、通常、蓄積装置等に備えられる記録媒体上の任意の位置から、蓄積したコンテンツの再生が可能であるので、従来のプレビュー機能を利用すると、コンテンツの内容として重要な部分のみ短時間に視聴することができ、蓄積したコンテンツが有料コンテンツであっても課金されることなく視聴されてしまうという問題があるからである。つまり、コンテンツを再生させる際の再生位置（再生箇所）に応じて、より細かくプレビュー制御できるものが望まれている。

【００１２】

そこで、本発明の目的は前記した従来の技術が有する課題を解消し、蓄積再生時に、プレビューを視聴することができ、また、編集または制作したプレビュー用コンテンツを取り扱うことができ、さらに、プレビュー再生時間を制御するこ

とができ、さらにまた、より細かくプレビュー制御できるコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムを提供することにある。

【００１３】

【課題を解決するための手段】

本発明は、前記した目的を達成するため、以下に示す構成とした。

請求項１記載のコンテンツ送信方法は、受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行うコンテンツ送信方法であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理ステップと、前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間情報を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化ステップと、前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力ステップと、を含むことを特徴とする。

【００１４】

この方法によれば、まず、コンテンツ暗号化ステップにおいて、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。続いて、コンテンツ送出管理ステップにおいて、異なる視聴形態により受信側で視聴させる場合の経過時間とコンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報が生成される。そして、第一暗号鍵暗号化ステップにおいて、第一鍵を含む関連情報およびコンテンツ経過時間情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。また、第二暗号鍵暗号化ステップにおいて、第二暗号鍵を含む関連情報および受信側におけるコンテンツとの利用を制御

する情報であるコンテンツ利用制御情報が第三暗号鍵で暗号化され、第二暗号鍵関連情報とされる。その後、多重出力ステップにおいて、暗号化コンテンツと、第一暗号鍵関連情報と、第二暗号化鍵関連情報とが多重化されて多重暗号化コンテンツとして出力される。

【００１５】

なお、異なる視聴形態とは、コンテンツの特定部分に加えられている制限がそれ以外の部分と異なっていたり、当該特定部分の経過時間が実時間と異なるように設定することで、コンテンツを送信する送信側の意図を反映させ、受信側におけるコンテンツの特定部分の視聴の形態が通常のコンテンツと異なるように規定されたものであり、例えば、プレビュー等である。

【００１６】

第一暗号鍵を含む関連情報とは、第一暗号鍵と、コンテンツを提供した事業者ＩＤ、つまり放送局、コンテンツ制作会社等の識別情報や、コンテンツ毎に付されているコンテンツＩＤ、つまり、コンテンツの識別情報等を含む情報である。第二暗号鍵を含む関連情報とは、第二暗号鍵と、コンテンツを提供した事業者ＩＤ、つまり放送局、コンテンツ制作会社等の識別情報や、コンテンツ毎に付されているコンテンツＩＤ、つまり、コンテンツの識別情報や、第三暗号鍵に付されている識別情報等を含む情報である。

【００１７】

また、通常、受信側の限定した受信者のみが視聴できるように、送信側でコンテンツを処理することを「スクランブルする」というが、ここでは、「暗号化する」という文言で統一的に表現している。

【００１８】

さらに、第一暗号鍵は、例えば、経過時間と共に数秒単位で変更されるスクランブル鍵を指すものであり、第二暗号鍵は、例えば、コンテンツ毎に設けられているコンテンツ鍵を指すものであり、第三暗号鍵は、例えば、コンテンツの継続時間よりも長時間保持されるワーク鍵を指すものである。

【００１９】

さらにまた、コンテンツ経過時間情報は、受信側で通常の視聴形態と異なる視

聴形態により視聴させる場合の経過時間について、コンテンツの実際の再生時間をもとに、コンテンツの内容（重要なシーン、重要でないシーン等）を参照して、付与した時間情報であり、例えば、コンテンツの再生時間と等しく付与したり、コンテンツの内容において重要なシーンの区間では、実際の再生時間よりも細かく付与したり、つまり、実際の再生時間が１分である場合にコンテンツ経過時間を２分として付与するものである。

【００２０】

コンテンツ利用制御情報とは、受信側でコンテンツを利用（視聴）する際に制御を規定した情報であり、例えば、コンテンツを利用できる有効期限、コンテンツの中でプレビュー許可した箇所を時刻によって指定したプレビュー開始時刻・終了時刻、プレビュー可能な合計時間を規定したプレビュー再生許可時間、コンテンツが有料か無料かを示すと共に、コンテンツが有料である場合に受信側の視聴者が購入したか借用したかを示す購入フラグ等が挙げられる。なお、このコンテンツ利用制御情報は、第二暗号鍵を含む関連情報と共に、暗号化しているが、第一暗号鍵を含む関連情報と共に、暗号化してもよい。ただし、コンテンツ利用制御情報を、第一暗号鍵を含む関連情報と共に暗号化すると、受信側で、暗号化コンテンツを復号化する際に、第一暗号鍵を含む関連情報が頻繁に復号化されるので、処理速度の低下を招き、最適とはいえない。

【００２１】

請求項２記載のコンテンツ送信装置は、受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行うコンテンツ送信装置であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理手段と、前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する

情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化手段と、前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力手段と、を備えることを特徴とする。

【００２２】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化される。コンテンツ送出管理手段で、異なる視聴形態により受信側で視聴させる場合の経過時間とコンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報が生成される。第一暗号鍵暗号化手段で、第一鍵を含む関連情報およびコンテンツ経過時間情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。第二暗号鍵暗号化手段で、第二暗号鍵を含む関連情報および受信側におけるコンテンツの利用を制御する情報であるコンテンツ利用制御情報が第三暗号鍵で暗号化され、第二暗号鍵関連情報とされる。多重出力手段で、暗号化コンテンツと、第一暗号鍵関連情報と、第二暗号化鍵関連情報とが多重化されて多重暗号化コンテンツとして出力される。

【００２３】

請求項３記載のコンテンツ送信装置は、請求項２に記載のコンテンツ送信装置において、前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間に対応する値として関連付けることを特徴とする。

【００２４】

かかる構成によれば、コンテンツ送出管理手段で、異なる視聴形態として受信側で視聴させる場合の経過時間が、コンテンツの開始時刻から連続して再生した場合の再生時間に対応する値として、コンテンツ経過時間情報が生成されるので、プレビュー機能を備えた装置を有する受信側では、単純に、コンテンツの再生時間に対応するプレビューを生成できる。

【００２５】

請求項４記載のコンテンツ送信装置は、請求項２に記載のコンテンツ送信装置において、前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間とは異なる不均一な値として関連付けることを特徴と

する。

【００２６】

かかる構成によれば、コンテンツ送出管理手段で、異なる視聴形態として受信側で視聴させる場合の経過時間が、コンテンツの開始時刻から連続して再生した場合の再生時間に不均一な値として、コンテンツ経過時間情報が生成される。つまり、コンテンツ経過時間情報が実際の再生時間によるものではなく、コンテンツの内容に応じて、異なる値に指定されている。このため、例えば、プレビュー機能を備えた装置を有する受信側では、送信側の意図（放送局等のコンテンツを制作した制作者の意図）に合わせたコンテンツのプレビューの制御が容易に実現される。

【００２７】

請求項５記載のコンテンツ送信装置は、請求項２に記載のコンテンツ送信装置において、前記コンテンツ送出管理手段は、前記コンテンツ経過時間情報を、前記経過時間が前記再生時間に対して増減した値として関連付けることを特徴とする。

【００２８】

かかる構成によれば、コンテンツ送出管理手段で、異なる視聴形態として受信側で視聴させる場合の経過時間が、コンテンツの開始時刻から連続して再生した場合の再生時間に対して増減した値として、コンテンツ経過時間情報が生成される。つまり、コンテンツ経過時間情報が実際の再生時間によるものではなく、コンテンツの各時点での内容に応じて、増減した値に指定される。このため、例えば、コンテンツのハイライトの部分では、短時間でプレビューの時間が終了してしまうように送信側で設定しておけば、プレビュー機能を備えた装置を有する受信側の視聴者は、コンテンツの全体を視聴したいとの欲求が高まり、この結果、コンテンツの購買意欲を増進させることができる。

【００２９】

請求項６記載のコンテンツ送信装置は、請求項２から請求項５のいずれか１項に記載のコンテンツ送信装置において、前記コンテンツの先頭に、予め、当該コンテンツの任意部分を取り出した試視聴用のプレビュー用コンテンツを配置し、

このプレビュー用コンテンツを前記第二暗号化鍵で暗号化するプレビュー用コンテンツ付加手段を備えたことを特徴とする。

【００３０】

かかる構成によれば、プレビュー用コンテンツ付加手段で、コンテンツの先頭に、当該コンテンツの任意の部分を取り出したプレビュー用コンテンツが配置され、このプレビュー用コンテンツが第二暗号鍵で暗号化される。これにより、プレビュー機能を備えた装置を有する受信側の視聴者に、送信者側の意図に応じたプレビュー用コンテンツを視聴させることができる。

【００３１】

請求項７記載のコンテンツ送信装置は、請求項２から請求項６のいずれか１項に記載のコンテンツ送信装置において、前記コンテンツを受信側で購入または借用された場合に料金を徴収する有料コンテンツである場合、前記受信側で当該有料コンテンツを購入または借用したかどうかを判定する購入フラグを前記コンテンツ利用制御情報内に設定する購入フラグ設定手段を備え、前記有料コンテンツが前記受信側で購入または借用された場合に受信側から返信される購入フラグに基づいて、前記有料コンテンツの徴収料金を確認する有料コンテンツ徴収料金確認手段を備えたことを特徴とする。

【００３２】

かかる構成によれば、コンテンツが有料コンテンツである場合、購入フラグ設定手段で、当該有料コンテンツを購入または借用したかどうかを判定する購入フラグがコンテンツ利用制御情報内に設定される。そして、プレビュー機能を備えた装置を有する受信側で有料コンテンツが購入された場合または借用された場合には購入フラグの値が変更され返信され、これにより、有料コンテンツ徴収料金確認手段で有料コンテンツの徴収料金が確認される。

【００３３】

請求項８記載のコンテンツ送信装置は、請求項２から請求項７のいずれか１項に記載のコンテンツ送信装置において、前記多重出力手段が、前記第二暗号鍵関連情報を、前記暗号化コンテンツおよび前記第一暗号鍵関連情報に多重化せずに、前記受信側からの要求に基づいて前記第二暗号鍵関連情報を出力することを特

徴とする。

【００３４】

かかる構成によれば、多重出力手段で、第二暗号鍵関連情報を多重化させずに、受信者側の要求に基づいて第二暗号鍵関連情報が出力される。つまり、この第二暗号鍵関連情報が暗号化コンテンツとは別に、送信されることになり、暗号化コンテンツをコンテンツに復号化して視聴したい場合に、受信側から送信側に要求が出され、第二暗号鍵関連情報が、例えば、通信回線網等を介して出力される。

【００３５】

請求項９記載のコンテンツ送信プログラムは、受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出し同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする管理を行う装置、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記異なる視聴形態により前記受信側で視聴させる場合の経過時間と前記コンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報を生成し、コンテンツの送出を管理するコンテンツ送出管理手段、前記第一暗号鍵を含む関連情報および前記コンテンツ経過時間情報を第二暗号鍵で暗号化して第一暗号鍵関連情報とする第一暗号鍵暗号化手段、前記第二暗号鍵を含む関連情報および前記受信側における前記コンテンツの利用を制御する情報であるコンテンツ利用制御情報を第三暗号鍵で暗号化して第二暗号鍵関連情報とする第二暗号鍵暗号化手段、前記暗号化コンテンツと、前記第一暗号鍵関連情報と、前記第二暗号鍵関連情報とを多重化して多重暗号化コンテンツとして出力する多重出力手段、である。

【００３６】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化される。コンテンツ送出管理手段で、異なる視聴形態により受信側で視聴させる場合の経過時間とコンテンツの開始時刻から連続して再生した場合の再生時間とを関連付けるコンテンツ経過時間情報が生成される。第一暗号鍵暗号化手段

で、第一鍵を含む関連情報およびコンテンツの経過時間情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。第二暗号鍵暗号化手段で、第二暗号鍵を含む関連情報および受信側におけるコンテンツの利用を制御した情報であるコンテンツ利用制御情報が第三暗号鍵で暗号化され、第二暗号鍵関連情報とされる。多重出力手段で、暗号化コンテンツと、第一暗号鍵関連情報と、第二暗号化鍵関連情報とが多重化されて多重暗号化コンテンツとして出力される。

【００３７】

請求項１０記載のコンテンツ受信方法は、請求項１記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にするコンテンツ受信方法であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離ステップと、この受信分離ステップにて分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄積装置に蓄積する暗号化コンテンツ蓄積ステップと、前記第二暗号鍵関連情報を、送信側に備えられている第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得ステップと、前記蓄積装置に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得ステップにて取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得ステップと、前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定ステップと、この視聴可能判定ステップにおける判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力ステップと、を含むことを特徴とする。

【００３８】

この方法によれば、まず、受信分離ステップにおいて、送信側から送信された多重暗号化コンテンツが受信され、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報が分離される。暗号化コンテンツ蓄積ステップにおいて、暗号化コンテンツおよび第一暗号鍵関連情報が蓄積装置に蓄積される。続いて、利用制御情報第二暗号鍵取得ステップにおいて、第二暗号鍵関連情報が第三暗号鍵で復号化され、コンテンツ利用制御情報および第二暗号鍵が取得される。そして、経過時間情報第一暗号鍵取得ステップにおいて、第一暗号鍵関連情報が第二暗号鍵で復号化され、コンテンツ経過時間情報および第一暗号鍵が取得される。その後、視聴可能判定ステップにおいて、コンテンツ経過時間情報に含まれる経過時間に基づき、異なる視聴形態による再生時間およびコンテンツ利用制御情報で規定される視聴可能条件に基づいて、暗号化コンテンツの特定部分を視聴可能か判定され、判定結果に基づいて、コンテンツ復号化出力ステップにおいて、暗号化コンテンツの特定部分が第一暗号鍵で復号化されて異なる視聴形態に出力される。

【００３９】

ここでは、便宜上、第一暗号鍵、第二暗号鍵および第三暗号鍵で復号化されるといった表現を使用しているが、実際には、第一暗号鍵、第二暗号鍵および第三暗号鍵は、例えば、スクランブル鍵、コンテンツ鍵、ワーク鍵等と表現されるものである。

【００４０】

請求項１１記載のコンテンツ受信装置は、請求項２記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にするコンテンツ受信装置であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離手段と、この受信分離手段で分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄積する暗号化コンテンツ蓄積手段と、前記第二暗号鍵関連情報を、送信側に備えられて

いる第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得手段と、前記暗号化コンテンツ蓄積手段に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得手段で取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得手段と、前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定手段と、この視聴可能判定手段における判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力手段と、を備えることを特徴とする。

【００４１】

かかる構成によれば、受信分離手段で、送信側から送信された多重暗号化コンテンツが受信され、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報が分離される。暗号化コンテンツ蓄積手段で、暗号化コンテンツおよび第一暗号鍵関連情報が蓄積される。続いて、利用制御情報第二暗号鍵取得手段で、第二暗号鍵関連情報が第三暗号鍵で復号化され、コンテンツ利用制御情報および第二暗号鍵が取得される。そして、経過時間情報第一暗号鍵取得手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、コンテンツ経過時間情報および第一暗号鍵が取得される。その後、視聴可能判定手段で、コンテンツ経過時間情報に含まれる経過時間に基づき、異なる視聴形態による再生時間およびコンテンツ利用制御情報で規定される視聴可能条件に基づいて、暗号化コンテンツの特定部分を視聴可能か判定され、判定結果に基づいて、コンテンツ復号化出力手段で、暗号化コンテンツの特定部分が第一暗号鍵で復号化され異なる視聴形態に出力される。

【００４２】

請求項１２記載のコンテンツ受信装置は、前記暗号化コンテンツを前記第一暗号鍵で復号化して再生した再生時間をカウントする再生時間カウント手段と、前

記コンテンツ利用制御情報に設定されている購入フラグを管理し、当該購入フラグにより前記暗号化コンテンツが有料である場合、前記再生時間カウント手段によってカウントした再生時間に応じて課金する課金手段とを備え、前記視聴可能判定手段は、前記再生時間と、前記コンテンツ利用制御情報に含まれる予め指定された再生許可時間とを比較判定し、この比較判定に基づき、前記課金手段は、前記再生時間が前記再生許可時間を経過するまで課金しないことを特徴とする。

【００４３】

かかる構成によれば、再生時間カウント手段で、暗号化コンテンツを第一暗号鍵で復号化して再生した再生時間がカウントされる。課金手段で、コンテンツ利用制御情報に設定されている購入フラグが管理され、当該購入フラグにより暗号化コンテンツが有料である場合、再生時間カウント手段でカウントされた再生時間に応じて課金される。ただし、例外的に、視聴可能判定手段で、再生時間とコンテンツ利用制御情報に含まれる予め指定された再生許可時間とが比較判定された判定結果に基づき、再生時間が再生許可時間を経過するまでは、課金手段で課金されない。

【００４４】

なお、再生時間カウント手段でカウントされた再生時間が、再生許可時間を超過した場合には、自動的に（強制的に）異なる視聴形態の再生が停止される。また、再生許可時間は、送信側の意図に応じて設定可能なものであり、或いは、コンテンツＩＤによって分類されるコンテンツの属性（短時間のコンテンツ、長時間のコンテンツ等）により、例えば、１分未満、１分以上３分未満、３分以上５分未満といったように区分けされているものである。

【００４５】

請求項１３記載のコンテンツ受信装置は、請求項１２に記載のコンテンツ受信装置において、前記再生時間カウント手段は、前記暗号化コンテンツの特定部分を異なる視聴形態でノンリニア再生した再生時間を、前記第一暗号鍵関連情報に含まれている前記第一暗号鍵が変更される変更単位時間に対応して付される連続指標に基づいて、カウントすることを特徴とする。

【００４６】

かかる構成によれば、再生時間カウント手段で、第一暗号鍵関連情報に含まれている前記第一暗号鍵が変更される変更単位時間に対応して付される連続指標に基づいて、ノンリニア再生した再生時間がカウントされる。ノンリニア再生は、いわゆる不連続な再生（スキップ再生等）のことであり、再生時間カウント手段で、連続指標により、例えば、スキップ再生時の不連続点を検出してスキップしている間のカウント時間を０秒とし、実際に再生した再生時間のみがカウントされる。

【００４７】

請求項１４記載のコンテンツ受信装置は、請求項１２または請求項１３に記載のコンテンツ受信装置において、記憶した情報が外部より読みとり不可能なセキュリティモジュールを備え、前記視聴可能判定手段による前記再生時間と前記再生許可時間との比較判定を、前記セキュリティモジュールの内部で行うことを特徴とする。

【００４８】

かかる構成によれば、記憶した情報が外部より読みとり不可能なセキュリティモジュールが備えられ、このセキュリティモジュールの内部で視聴可能判定手段による再生時間と再生許可時間との比較判定が行われる。つまり、セキュリティモジュールの内部であれば、再生時間と、再生許可時間との双方が改ざんされるおそれがなく、比較判定が実行できる。なお、セキュリティモジュールは、ＩＣカード等で構成されるものである。

【００４９】

請求項１５記載のコンテンツ受信装置は、請求項１４に記載のコンテンツ受信装置において、前記セキュリティモジュールの内部で、前記第二暗号鍵関連情報を扱う場合、前記課金手段で、前記暗号化コンテンツを識別する識別子であるコンテンツＩＤ毎に、前記第二暗号鍵関連情報に含まれているコンテンツ利用制御情報を関連付け、前記再生時間カウント手段でカウントした再生時間を、前記コンテンツ利用制御情報に含めたコンテンツ履歴情報とすることを特徴とする。

【００５０】

かかる構成によれば、セキュリティモジュールの内部で、第二暗号鍵関連情報

が扱われる場合、課金手段で、暗号化コンテンツを識別する識別子であるコンテンツＩＤ毎に、第二暗号鍵関連情報に含まれているコンテンツ利用制御情報が関連付けられ、再生時間カウント手段でカウントされた再生時間が含められ、コンテンツ履歴情報とされる。

【００５１】

請求項１６記載のコンテンツ受信装置は、請求項１５に記載のコンテンツ受信装置において、前記視聴可能判定手段で前記再生時間と前記再生許可時間との比較判定した判定結果、前記再生時間が前記再生許可時間に達していない場合、前記コンテンツ履歴情報および前記第二暗号鍵を含む関連情報を前記セキュリティモジュールの内部に備えられる固有鍵で再暗号化した再暗号化第二暗号鍵関連情報とし、この再暗号化第二暗号鍵関連情報を前記暗号化コンテンツ蓄積手段に記憶させる再暗号化手段を備えることを特徴とする。

【００５２】

かかる構成によれば、視聴可能判定手段で再生時間と再生許可時間とを比較判定した判定結果、再生時間が再生許可時間に達していない場合、再暗号化手段で、コンテンツ履歴情報および第二暗号鍵を含む関連情報がセキュリティモジュールの内部に備えられる固有鍵で再暗号化され、再暗号化第二暗号鍵関連情報とされる。そして、この再暗号化第二暗号鍵関連情報が暗号化コンテンツ蓄積手段に記憶される。通常、暗号化コンテンツを蓄積させる暗号化コンテンツ蓄積手段は、セキュリティモジュールの外部にあり、コンテンツ履歴情報および第二暗号鍵の改ざんを防止するため、再暗号化される。なお、セキュリティモジュール内部にコンテンツ履歴情報および第二暗号鍵を記憶させることができるレジスト機構（メモリー）が備えられていれば、このレジスト機能に記憶しておくことも可能である。

【００５３】

請求項１７記載のコンテンツ受信装置は、請求項１６に記載のコンテンツ受信装置において、前記第二暗号鍵関連情報を前記暗号化コンテンツと共に、前記暗号化コンテンツ蓄積手段に蓄積する場合、前記再暗号化手段で再暗号化して前記暗号化コンテンツ蓄積手段に記憶させることを特徴とする。

【００５４】

かかる構成によれば、第二暗号鍵関連情報を暗号化コンテンツと共に、暗号化コンテンツ蓄積手段に蓄積する場合、再暗号化手段で再暗号化されて暗号化コンテンツ蓄積手段に記憶される。通常、暗号化コンテンツを蓄積させる暗号化コンテンツ蓄積手段は、セキュリティモジュールの外部にあり、第二暗号鍵関連情報の改ざんを防止するため、再暗号化される。

【００５５】

請求項１８記載のコンテンツ受信装置は、請求項１２から請求項１７のいずれか１項に記載のコンテンツ受信装置において、前記課金手段は、前記有料コンテンツを購入するか借用するかに関する情報を、通信回線網を介して、前記コンテンツ送信装置に通知することを特徴とする。

【００５６】

かかる構成によれば、課金手段で有料コンテンツを購入するか借用するかに関する情報が、通信回線網を介して、コンテンツ送信装置に通知される。これにより、コンテンツ送信装置側のコンテンツ提供者（放送局等の事業者）は、有料コンテンツにかかる料金を確認することができる。

【００５７】

請求項１９記載のコンテンツ受信装置は、請求項１２から請求項１８のいずれか１項に記載のコンテンツ受信装置において、前記多重暗号化コンテンツに前記第二暗号鍵関連情報が多重化されていない場合、前記第二暗号鍵関連情報を、通信回線網を介して前記コンテンツ送信装置に要求する第二暗号鍵関連情報要求手段を備え、前記暗号化コンテンツが有料コンテンツである場合、前記課金手段が、前記第二暗号鍵関連情報を取得する際に、前記有料コンテンツにかかる料金を課金することを特徴とする。

【００５８】

かかる構成によれば、受信した多重暗号化コンテンツに第二暗号鍵関連情報が多重化されていない場合、第二暗号鍵関連情報要求手段で、第二暗号鍵関連情報が通信回線網を介してコンテンツ送信装置に要求される。なおかつ、暗号化コンテンツが有料コンテンツである場合、課金手段で、第二暗号鍵関連情報が取得さ

れる際に、有料コンテンツにかかる料金が課金される。

【００５９】

請求項２０記載のコンテンツ受信プログラムは、請求項９記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツを蓄積後、当該暗号化コンテンツの特定部分を復号化し、同暗号化コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にする装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報を分離する受信分離手段、この受信分離手段で分離した暗号化コンテンツおよび第一暗号鍵関連情報を蓄積する暗号化コンテンツ蓄積手段、前記第二暗号鍵関連情報を、送信側に備えられている第三暗号鍵と同様の第三暗号鍵で復号化し、前記第二暗号鍵関連情報に含まれるコンテンツ利用制御情報および第二暗号鍵を取得する利用制御情報第二暗号鍵取得手段、前記暗号化コンテンツ蓄積手段に蓄積されている第一暗号鍵関連情報を前記利用制御情報第二暗号鍵取得手段で取得された第二暗号鍵で復号化し、前記第一暗号鍵関連情報に含まれるコンテンツ経過時間情報および第一暗号鍵を取得する経過時間情報第一暗号鍵取得手段、前記コンテンツ経過時間情報に含まれる経過時間に基づき、前記異なる視聴形態による再生時間および前記コンテンツ利用制御情報で規定される視聴可能条件に基づいて、前記暗号化コンテンツの特定部分を視聴可能か判定する視聴可能判定手段、この視聴可能判定手段における判定結果に基づいて、前記暗号化コンテンツの特定部分を前記第一暗号鍵で復号化し、異なる視聴形態に出力するコンテンツ復号化出力手段、である。

【００６０】

かかる構成によれば、受信分離手段で、送信側から送信された多重暗号化コンテンツが受信され、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報が分離される。暗号化コンテンツ蓄積手段で、暗号化コンテンツおよび第一暗号鍵関連情報が蓄積される。続いて、利用制御情報第二暗号鍵取得手段で、第二暗号鍵関連情報が第三暗号鍵

で復号化され、コンテンツ利用制御情報および第二暗号鍵が取得される。そして、経過時間情報第一暗号鍵取得手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、コンテンツ経過時間情報および第一暗号鍵が取得される。その後、視聴可能判定手段で、コンテンツ経過時間情報に含まれる経過時間に基づき、異なる視聴形態による再生時間およびコンテンツ利用制御情報で規定される視聴可能条件に基づいて、暗号化コンテンツの特定部分を視聴可能か判定され、判定結果に基づいて、コンテンツ復号化出力手段で、暗号化コンテンツの特定部分が第一暗号鍵で復号化され、異なる視聴形態に出力される。

【００６１】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。

この実施の形態における説明の順序について述べると、まず、コンテンツ送信装置の構成、コンテンツ受信装置の構成について説明し、次に、コンテンツ送信装置の動作、コンテンツ受信装置の動作について説明する。そして、コンテンツ経過時間情報について説明し、また、プレビュー再生時間の計測の仕方（後記する再生時間カウンタ部の演算方式）について説明し、さらに、コンテンツ利用制御情報とコンテンツ履歴情報とについて説明し、さらにまた、プレビュー用コンテンツが予め付加されているコンテンツについて、従来のコンテンツと比較しつつ説明する。

【００６２】

（コンテンツ送信装置の構成）

コンテンツ送信装置の構成について図１を参照して説明する。図１は、コンテンツ送信装置のブロック図であり、この図１に示すように、コンテンツ送信装置１は、ＭＰＥＧ２エンコード部３と、スクランブル部５と、ＥＣＭ－Ｋｗ生成部７と、コンテンツ送出管理部９と、ＥＣＭ－Ｋｃ生成部１１と、Ｋｃ配布用ＥＣＭ生成部１３と、多重化部１５とを備えている。

【００６３】

コンテンツ送信装置１は、入力されたコンテンツ（番組、映像音声Ｍａｖ［ｍｅｓｓａｇｅ　ａｕｄｉｏ　ｖｉｓｕａｌ］）を、送信（送出）先の受信側（コ

ンテンツ受信装置（詳細は後記する））で当該コンテンツの任意部分（任意箇所）を送信側の意図に応じて、プレビュー（異なる視聴形態）が可能なように処理してから、当該コンテンツを暗号化して送信するものである。なお、このコンテンツ送信装置１は、主に有料コンテンツを送信して、この有料コンテンツを受信したコンテンツ受信装置の所有者が当該有料コンテンツを視聴または購入或いは借用した場合に、課金することができるように構成されている。

【００６４】

また、コンテンツを送信する送信側（コンテンツ送信装置１）の意図を、コンテンツを受信する受信側に反映させるために、コンテンツ送信装置１は、当該コンテンツと共に、コンテンツ利用制御情報を送信するように構成されている。ここで、コンテンツ利用制御情報について説明しておく。

コンテンツ利用制御情報は、有効期限、プレビュー開始時刻・終了時刻、プレビュー再生許可時間、購入フラグを含んで構成されている。

【００６５】

有効期限は、コンテンツを受信した受信側で利用（視聴等）することができる期限を示すものである。つまり、この有効期限は、後記するコンテンツ鍵Ｋｃの利用可能期限であるともいえるものである。

【００６６】

プレビュー開始時刻・終了時刻は、プレビューを許可する期間（時間）を示すものである。例えば、プレビュー開始時刻が１１時４０分（１１：４０）、プレビュー終了時刻が１１時４３分（１１：４３）と定義されており、この場合、プレビューが許可される時間は３分間ということになる。また、このプレビュー開始時刻・終了時刻は、プレビュー可能な箇所を指定したものであるといえる。

【００６７】

プレビュー再生許可時間は、何秒間（場合よっては、何分間）プレビュー再生を許可するかを示すものである。例えば、３０秒と定義されており、この場合、プレビュー再生許可時間の合計時間が３０秒ということになり、コンテンツを受信して視聴する視聴者によっては、例えば、１０秒ずつ３回（合計３０秒）といったように、プレビュー再生を行うことができることになる。つまり、このプレ

ビュー再生許可時間は、送信側の意図に応じて設定可能なものであり、或いは、コンテンツＩＤによって分類されるコンテンツの属性（短時間のコンテンツ、長時間のコンテンツ等）により、例えば、１分未満、１分以上３分未満、３分以上５分未満といったように区分けされているものである。

【００６８】

購入フラグは、コンテンツが無料か有料かを示すと共に、コンテンツが有料である場合、コンテンツが購入されたか、一定期間、視聴者に借用されたか（レンタルされたか）を示すものである。例えば、購入フラグは、有料であり未購入の場合は「０」、有料であり購入済みの場合「１」、有料でありレンタル中である場合「２」、無料の場合「３」と定義されている。なお、図示を省略したが、コンテンツ送信装置１には、この購入フラグを設定する購入フラグ設定手段が備えられている。

【００６９】

これより、コンテンツ送信装置１の各構成を説明する。

ＭＰＥＧ２エンコード部３は、入力された映像音声コンテンツである映像音声Ｍａｖ（Ｍｅｓｓａｇｅ　ａｕｄｉｏ　ｖｉｓｕａｌ）を符号化（エンコード）して、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）を生成するものである。なお、エンコードとは、映像音声信号からデジタル符号を生成することであり、エンコードの目的は、アナログ信号をデジタル信号に変換することや、デジタル信号の冗長度を減らすことで、元の信号を圧縮して伝送または蓄積されるデータ量を減少させることや、誤り検出や訂正を可能にする等が挙げられる。

【００７０】

スクランブル部５は、ＭＰＥＧ２エンコード部３でエンコードされた映像音声コンテンツストリーム（ＴＳ）をスクランブル鍵Ｋｓでスクランブルして、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を生成するものである。このコンテンツ送信装置１には、スクランブル鍵Ｋｓを生成するスクランブル鍵生成手段（図示せず）が備えられている。スクランブルは、ストリーム形式の信号の暗号化を指すものであり、スクランブル鍵Ｋｓは、コンテンツの経過時間に伴い、数秒単位（一般的には１秒程度）で変更される暗号鍵である。なお、このスクランブル部５

が特許請求の範囲の請求項に記載したコンテンツ暗号化手段に相当するものであり、スクランブル鍵Ｋｓが第一暗号鍵に相当するものである。

【００７１】

ＥＣＭ－Ｋｗ生成部７は、スクランブル鍵Ｋｓと、現在時刻情報とをワーク鍵Ｋｗで暗号化して、受信側でリアルタイムに映像音声Ｍａｖを再生する時に用いられるリアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））を生成するものである。現在時刻情報は、現在の時刻から得られる情報であり、例えば、現在の時刻が２００２年８月２６日午後８時３０分１６秒であれば、現在時刻情報は、「０２／０８／２６　２０：３０：１６」となるものである。

【００７２】

リアルタイム受信時用第一暗号鍵関連情報は、いわゆるＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ：暗号化関連情報）であり、このリアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））は、受信側のコンテンツ受信装置でリアルタイムに暗号化コンテンツを復号化する際に用いられるものである。ワーク鍵Ｋｗは、送信側であるコンテンツ送信装置１と受信側であるコンテンツ受信装置（後記）との間で、長期間にわたり共通に保持される暗号鍵である。なお、ワーク鍵Ｋｗが特許請求の範囲の請求項に記載した第三暗号鍵に相当するものである。

【００７３】

コンテンツ送出管理部９は、コンテンツ経過時間情報および連続指標をＥＣＭ－Ｋｃ生成部１１に出力すると共に、コンテンツ送出情報を多重化部１５に出力するものである。コンテンツ経過時間情報は、コンテンツに付加されるものであって、当該コンテンツの冒頭を０秒にして、コンテンツの経過時間に伴い、コンテンツの内容に応じて、規則的にまたは不規則的に増加していく時間に関する情報である。詳細は後記する。なお、このコンテンツ送出管理部９が特許請求の範囲の請求項に記載したコンテンツ送出管理手段に相当するものである。

【００７４】

連続指標は、スクランブル鍵Ｋｓが変更される変更単位時間（数秒単位（一般的には１秒程度））に対応して、コンテンツに付される時間情報（経過時間）で

ある。コンテンツ送出情報は、ＥＩＴ（Ｅｖｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）や、ＳＤＴ（Ｓｅｒｖｉｃｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｔａｂｌｅ）等であり、受信側のコンテンツ受信装置でＥＰＧ（電子番組表）等を作成する際に供される情報である。

【００７５】

ＥＣＭ－Ｋｃ生成部１１は、スクランブル鍵Ｋｓを含む関連情報と、コンテンツ経過時間情報とを、コンテンツ鍵Ｋｃで暗号化して、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））を生成するものである。スクランブル鍵Ｋｓを含む関連情報は、スクランブル鍵Ｋｓと、コンテンツを提供した事業者ＩＤ、コンテンツ毎に付されているコンテンツＩＤ等である。

【００７６】

コンテンツ鍵Ｋｃは、コンテンツ毎に個別に設けられる暗号鍵である。第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））は、受信側のコンテンツ受信装置で暗号化コンテンツを蓄積した後、再生する際（蓄積再生時）に当該暗号化コンテンツを復号化する際に用いられるものである。なお、このＥＣＭ－Ｋｃ生成部１１が特許請求の範囲の請求項に記載した第一暗号鍵暗号化手段に相当するものであり、コンテンツ鍵Ｋｃが第二暗号鍵に相当するものである。

【００７７】

Ｋｃ配布用ＥＣＭ生成部１３は、コンテンツ鍵Ｋｃを含む関連情報と、コンテンツ利用制御情報とをワーク鍵Ｋｗで暗号化して、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））を生成するものである。コンテンツ鍵Ｋｃを含む関連情報は、コンテンツ鍵Ｋｃと、コンテンツを提供した事業者ＩＤ、コンテンツ毎に付されているコンテンツＩＤ、ワーク鍵Ｋｗに付されている識別情報等を含む情報である。なお、コンテンツ鍵Ｋｃを含む関連情報と、コンテンツ利用制御情報とを合わせて、Ｋｃ配布用ＥＣＭと呼称することにする。

【００７８】

第二暗号鍵関連情報は、受信側のコンテンツ受信装置で暗号化コンテンツからプレビューを行うために用いられるものである。なお、このＫｃ配布用ＥＣＭ生成部１３が特許請求の範囲の請求項に記載した第二暗号鍵暗号化手段に相当する

ものである。

【００７９】

多重化部１５は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、リアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））と、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とを多重化した多重暗号化コンテンツをＭＰＥＧ２トランスポートストリーム形式で送出するものである。

【００８０】

また、この多重化部１５は、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））のみを多重化させずに、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、リアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））と多重化した多重暗号化コンテンツをＭＰＥＧ２トランスポートストリーム形式で送出可能に構成されている。つまり、多重化部１５は、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））のみを、任意の時間に送出したり、受信側からの要求に基づいて通信回線網（図示せず）を介して送出したりできるように構成されている。なお、この多重化部１５が特許請求の範囲の請求項に記載した多重出力手段に相当するものである。

【００８１】

さらに、このコンテンツ送信装置１には、映像音声Ｍａｖ（コンテンツ）の先頭に、予め、当該映像音声Ｍａｖ（コンテンツ）の任意部分を取り出した試視聴用のプレビュー用コンテンツを配置して、このプレビュー用コンテンツをコンテンツ鍵Ｋｃで暗号化するプレビュー用コンテンツ付加手段（図示せず）が備えられている。このプレビュー用コンテンツ付加手段（図示せず）で付加されたプレビュー用コンテンツは、後記するコンテンツ受信装置で、取得されたコンテンツ鍵Ｋｃで復号化され、コンテンツ受信装置の使用者（視聴者）に視聴される。このため、コンテンツ送信側の意図に応じたプレビューを、映像音声Ｍａｖ（コンテンツ）を視聴しようとした視聴者に視聴させることができる。

【００８２】

さらにまた、このコンテンツ送信装置１には、当該コンテンツ送信装置１に入

力された映像音声Ｍａｖが有料コンテンツであり、この有料コンテンツが受信側で購入または借用された場合に受信側から返信される購入フラグに基づいて、有料コンテンツの徴収料金を確認する有料コンテンツ徴収料金確認手段（図示せず）が備えられている。この有料コンテンツ徴収料金確認手段で、コンテンツを送信した送信側では、例えば、後記するコンテンツ受信装置を使用する使用者（視聴者）宅を定期的に訪問する等して、有料コンテンツの徴収料金を確認する必要がなくなる。つまり、当該コンテンツ送信装置１の利便性を向上させることができる。

【００８３】

このコンテンツ送信装置１によれば、スクランブル部５で、映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵Ｋｓでスクランブルされ、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））とされる。ＥＣＭ－Ｋｃ生成部１１で、スクランブル鍵Ｋｓを含む関連情報と、コンテンツ経過時間情報とがコンテンツ鍵Ｋｃで暗号化され、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とされる。Ｋｃ配布用ＥＣＭ生成部１３で、コンテンツ鍵Ｋｃを含む関連情報がワーク鍵Ｋｗで暗号化され、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とされる。多重化部１５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））と、第二暗号化鍵関連情報Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とが多重化されて多重暗号化コンテンツとして出力される。このため、プレビュー機能を備えたコンテンツ受信装置で、この多重暗号化コンテンツが受信されれば、コンテンツ経過時間情報に基づいて、プレビューを生成（制作）でき、コンテンツ利用制御情報に基づいて、再生時間が制御されたプレビューを視聴することができる。

【００８４】

映像音声Ｍａｖが有料である場合、購入フラグ設定手段（図示せず）で、当該有料コンテンツを購入または借用したかどうかを判定する購入フラグが第二暗号化鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））内に設定される。そして、プレビュー機能を備えた装置を有する受信側で有料コンテンツが購入された場合には、購入フラグが変更されると共に、コンテンツ利用制御情報に含まれる有効期限

が無期限に、借用された場合にはコンテンツ利用制御情報に含まれる有効期限が有限に設定される。このため、受信側の視聴者が、有料コンテンツのプレビューを視聴して、当該有料コンテンツを購入したくなった場合や借用（レンタル）したくなった場合には、購入フラグの設定を変更することによって、即座に、有料コンテンツを視聴することができる。

【００８５】

多重化部１５で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））を多重化させずに、受信者側の要求に基づいて第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が出力される。つまり、この第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））とは別に、送信されることになり、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を映像音声Ｍａｖに復号化して視聴したい場合に、受信側から送信側に要求が出され、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が、例えば、通信回線網等を介して出力される。このため、受信側の視聴者が実際に映像音声Ｍａｖを視聴したかの如何に拘わらず、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））を出力した時点で、映像音声Ｍａｖを利用した（視聴した）とみなして、課金することができる。

【００８６】

（コンテンツ受信装置の構成）

次に、コンテンツ受信装置の構成について図２を参照して説明する。図２は、コンテンツ受信装置のブロック図であり、この図２に示すように、コンテンツ受信装置２１は、受信分離部２３と、コンテンツ蓄積部２５と、分離部２７と、セキュリティモジュール２９と、デスクランブル部３１と、ＭＰＥＧ２デコード部３３とを備えている。

【００８７】

コンテンツ受信装置２１は、送信側のコンテンツ送信装置１（図１）から送信された多重暗号化コンテンツを受信し、この多重暗号化コンテンツに多重化されている暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の任意部分（送信側で指定された部分）をプレビュー可能に処理して、当該暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋ

ｓ））を購入または借用した場合に課金可能に構成されるものである。

【００８８】

受信分離部２３は、送信側のコンテンツ送信装置１から送信された多重暗号化コンテンツを受信して、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とをコンテンツ蓄積部２５に出力すると共に、リアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））と、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とをセキュリティモジュール２９に出力するものである。なお、この受信分離部２３が特許請求の範囲の請求項に記載した受信分離手段に相当するものである。

【００８９】

コンテンツ蓄積部２５は、大容量のハードディスク等によって構成され、受信分離部２３から出力された暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とを蓄積すると共に、セキュリティモジュール２９（再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１）で再暗号化された再暗号化Ｋｃ配布用ＥＣＭを記録するものである。このコンテンツ蓄積部２５が特許請求の範囲の請求項に記載した暗号化コンテンツ蓄積手段に相当するものである。

【００９０】

分離部２７は、受信分離部２３で受信された多重暗号化コンテンツの暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とがコンテンツ蓄積部２５に蓄積された後に、再生させる蓄積再生時に、これら暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とを分離するためのものであり、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））をデスクランブル部３１に出力すると共に、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））をセキュリティモジュール２９に出力するものである。

【００９１】

セキュリティモジュール２９は、ＩＣカード等によって構成され、内部に記録した情報を外部より読み取り不可能に構成されたものであり、ＥＣＭ－Ｋｃ解析

部３５と、ＥＣＭ－Ｋｗ解析部３７と、Ｋｃ配布用ＥＣＭ解析部３９と、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１と、Ｋｃ配布用ＥＭＭ解析部４３と、再生時間カウンタ部４５と、視聴プレビュー判定部４７と、送出制御部４９と、ＶｉｅｗＬｏｇ課金部５１とを備えている。

【００９２】

ＥＣＭ－Ｋｃ解析部３５は、蓄積再生時に機能するものであり、分離部２７から出力された第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））をコンテンツ鍵Ｋｃで復号化し、スクランブル鍵Ｋｓ、コンテンツ経過時間情報および連続指標を取得すると共に、スクランブル鍵Ｋｓを送出制御部４９に、コンテンツ経過時間情報を視聴プレビュー判定部４７に、連続指標を再生時間カウンタ部４５に出力するものである。このＥＣＭ－Ｋｃ解析部３５で使用されるコンテンツ鍵Ｋｃは、Ｋｃ配布用ＥＣＭ解析部３９若しくは再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１またはＫｃ配布用ＥＭＭ解析部４３で取得されたものである。なお、このＥＣＭ－Ｋｃ解析部３５が特許請求の範囲の請求項に記載した経過時間情報第一暗号鍵取得手段に相当するものである。

【００９３】

ＥＣＭ－Ｋｗ解析部３７は、受信分離部２３で受信した多重暗号化コンテンツを受信しながらリアルタイムに再生するリアルタイム受信再生時に機能するものであり、受信分離部２３で分離されたリアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））を、送信側のコンテンツ送信装置１に保持されているものと同様のワーク鍵Ｋｗで復号化し、スクランブル鍵Ｋｓおよび現在時刻情報を取得すると共に、スクランブル鍵Ｋｓを送出制御部４９に、現在時刻情報を視聴プレビュー判定部４７に出力するものである。

【００９４】

Ｋｃ配布用ＥＣＭ解析部３９は、蓄積再生時に機能するものであり、受信分離部２３で分離された第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））をワーク鍵Ｋｗで復号化し、復号化されたＫｃ配布用ＥＣＭを再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１に出力すると共に、この復号化されたＫｃ配布用ＥＣＭからコンテンツ鍵Ｋｃおよびコンテンツ利用制御情報を取得し、コンテンツ鍵Ｋｃを

ＥＣＭ－Ｋｃ解析部３５に、コンテンツ利用制御情報を視聴プレビュー判定部４７に出力するものである。このＫｃ配布用ＥＣＭ解析部３９が特許請求の範囲の請求項に記載した利用制御情報第二暗号鍵取得手段に相当するものである。

【００９５】

なお、コンテンツ利用制御情報は、このセキュリティモジュール２９内部では、プレビューの再生時間等の情報が付加されて、映像音声Ｍａｖ（コンテンツ）毎に付されている識別情報であるコンテンツＩＤ毎にテーブルにまとめられたコンテンツ履歴情報として取り扱われる。

【００９６】

また、通常、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がデスクランブル部３１にてデスクランブルされるまで、Ｋｃ配布用ＥＣＭ解析部３９に備えられている記憶手段（図示せず）で記憶される（ストックされる）。

【００９７】

或いは、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））を暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と共に、コンテンツ蓄積部２５に蓄積する場合には、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１で再暗号化されてコンテンツ蓄積部２５に記憶される。

【００９８】

ここで補足しておくと、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））がコンテンツ蓄積部２５に記憶されるのに対し、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が通常、セキュリティモジュール２９のＫｃ配布用ＥＣＭ解析部３９に記憶されるのは、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））に比べ、圧倒的に記憶容量が少ないためである。これにより、コンテンツ受信装置２１（受信側）において、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がデスクランブル部３１にてデスクランされる際の負荷軽減がなされる。

【００９９】

また、このＫｃ配布用ＥＣＭ解析部３９には、受信した多重暗号化コンテンツ

に第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が多重化されていない場合、コンテンツ受信装置２１の使用者（視聴者）の意向に基づいて、通信回線網と介して、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））をコンテンツ送信装置１に要求する第二暗号鍵関連情報要求手段（図示せず）が備えられている。

【０１００】

再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１は、受信分離部２３に多重暗号化コンテンツが入力される都度、Ｋｃ配布用ＥＣＭ解析部３９で復号化されたＫｃ配布用ＥＣＭを再暗号化し、再暗号化Ｋｃ配布用ＥＣＭとしてコンテンツ蓄積部２５に逐次出力して、記憶させるものである。また、Ｋｃ配布用ＥＣＭ解析部３９で復号されたＫｃ配布用ＥＣＭ（コンテンツ鍵Ｋｃを含む関連情報およびコンテンツ利用制御情報）内のコンテンツ利用制御情報を、再生時間カウンタ部４５から出力される再生時間およびＶｉｅｗＬｏｇ課金部５１から出力される購入フラグの値と有効期限に基づいて修正し、固有鍵で再暗号化して再暗号化Ｋｃ配布用ＥＣＭ（請求項に記載した再暗号化第二暗号鍵関連情報に相当）を生成し、コンテンツ蓄積部２５に出力するものである。

【０１０１】

また、逆に、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１は、コンテンツ蓄積部２５に記憶した再暗号化Ｋｃ配布用ＥＣＭを再復号化して、再復号化した再復号化Ｋｃ配布用ＥＣＭからコンテンツ利用制御情報（再復号化されたコンテンツ利用制御情報）を視聴プレビュー判定部４７に出力するものである。なお、固有鍵はセキュリティモジュール２９毎に設定されている、固有（特有）の暗号鍵である。

【０１０２】

なお、この再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１は、セキュリティモジュール２９内部にレジスト機能（記録装置）が備えられている場合には、このレジスト機能で代用できるものである。つまり、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１は、セキュリティモジュール２９外部にＫｃ配布用ＥＣＭに含まれているコンテンツ鍵Ｋｃやコンテンツ利用制御情報等の重要な情報の盗用や改ざんを防

止するためのものである。また、この再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１が特許請求の範囲の請求項に記載した再暗号化手段に相当するものである。

【０１０３】

Ｋｃ配布用ＥＭＭ解析部４３は、送信側の放送局等から送られるＫｃ配布用ＥＭＭを、送信側と受信側とで共通の暗号鍵を用いる共通鍵暗号化方式による共通鍵で復号化し、コンテンツ鍵Ｋｃおよびコンテンツ利用制御情報を取得し、コンテンツ鍵ＫｃをＥＣＭ－Ｋｃ解析部３５に、コンテンツ利用制御情報を視聴プレビュー判定部４７に出力するものである。なお、この実施の形態では、Ｋｃ配布用ＥＭＭ解析部４３は通信回線網を介して、Ｋｃ配布用ＥＭＭを入手する構成となっている。

【０１０４】

つまり、Ｋｃ配布用ＥＭＭは、受信側のコンテンツ受信装置２１の使用者（視聴者）が送信側の放送局等に要求（注文）し、この要求（注文）に基づいて送信側から配信され、受信側で取得されるものである。送信側の放送局では、Ｋｃ配布用ＥＭＭの要求があった時点で暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が利用されたとみなして料金を課金することができる。つまり、Ｋｃ配布用ＥＭＭに含まれているコンテンツ利用制御情報の購入フラグが予め、購入または借用を示す値に設定されている。また、このＫｃ配布用ＥＭＭは、いわゆるＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ：個別関連情報）である。

【０１０５】

再生時間カウンタ部４５は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の一部分をプレビューした場合、プレビューした時間（請求項に記載した再生時間に相当）、つまり、映像音声Ｍａｖの再生時間を計測（カウント）するものであり、計測した再生時間情報を視聴プレビュー判定部４７および再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１に出力するものである。また、この再生時間カウンタ部４５は、プレビューした時間のみならず、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を視聴した視聴時間もカウントすることができるものである。

【０１０６】

この再生時間カウンタ部４５でカウントされた再生時間は、視聴プレビュー判定部４７で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））のプレビューが可能かどうか判定する際の判定要素の１つとなる。つまり、視聴プレビュー判定部４７では、再生時間と、コンテンツ利用制御情報に含まれているプレビュー再生許可時間（視聴許可条件の一つ、請求項に記載した再生許可時間に相当）と比較判定してプレビュー可能かどうかを判定するからである。

【０１０７】

例えば、再生時間がプレビュー再生許可時間よりも少なければ、まだプレビューすることができるし、プレビュー再生許可時間を超過していれば（超過した時点で）、プレビューすることができない。この再生時間カウンタ部４５における映像音声Ｍａｖ再生時間の計測の仕方（演算方式）についての詳細は後記する。なお、この再生時間カウンタ部４５が特許請求の範囲の請求項に記載した再生時間カウント手段に相当するものである。

【０１０８】

視聴プレビュー判定部４７は、視聴者の意向（判断）を参酌して、入力されたコンテンツ経過時間情報、現在時刻情報、コンテンツ利用制御情報および再生時間情報（視聴可能条件）に基づいて、プレビュー可能かどうかを判定（視聴可能判定）し、判定した結果である制御情報を送出制御部４９に出力すると共に、プレビューした場合の料金および購入または借用した場合の料金に関する課金情報と、購入フラグ（購入フラグの数値）および再設定された有効期限を含めたコンテンツ利用制御情報と、再生時間カウント部４５でカウントした再生時間とをＶｉｅｗＬｏｇ課金部５１に出力するものである。

【０１０９】

また、視聴プレビュー判定部４７は、視聴者の判断に基づいて、コンテンツ利用制御情報の購入フラグおよび有効期限の再設定を行うものである。なお、この視聴プレビュー判定部４７におけるプレビュー判定およびコンテンツ利用制御情報の購入フラグおよび有効期限の再設定についての詳細な説明は、後記する動作の説明で行うこととする。また、この視聴プレビュー判定部４７が特許請求の範囲の請求項に記載した視聴可能判定手段に相当するものである。

【０１１０】

例えば、制御情報は、コンテンツ受信装置２１の視聴者が暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を購入するまたは借用する（レンタルする）と判断して、図示を省略した当該装置２１の操作部に備えられる購入確認ボタン（借用確認ボタン）を押下した場合には、暗号化コンテンツＥ（Ｍａｖ，Ｋｓ））の全てを視聴可能なように全てのスクランブル鍵Ｋｓを送出制御部４９からセキュリティモジュール２９の外部に出力許可する情報（全スクランブル鍵Ｋｓ送出可）である。

【０１１１】

また、制御情報は、コンテンツ受信装置２１の視聴者が暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））のプレビューを所望する際に、図示を省略した当該装置２１の操作部に備えられるプレビュー実行ボタンを押下した場合には、プレビュー判定後、プレビュー可能であれば、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の一部を視聴可能なように一部のスクランブル鍵Ｋｓを送出制御部４９からセキュリティモジュール２９の外部に出力許可する情報（一部のスクランブル鍵Ｋｓ送出可）である。

【０１１２】

さらに、制御情報は、プレビュー判定の結果、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））のプレビューができないと判定された場合には、プレビューできない旨の情報（エラーコード）である。

【０１１３】

課金情報は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が無料の場合は、当然のことながら、“０円”となる。また、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が有料であり、視聴プレビュー判定部４７で当該暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の再生時間がプレビュー再生許可時間よりも短い場合には、通常は“０円”となる。なお、当該暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の再生時間がプレビュー再生許可時間よりも短い場合であっても、再生時間に応じて課金することは可能である。つまり、この場合、課金情報は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を再生させた数秒間でいくら（例えば、３秒間１０円）と設

定することになり、プレビュー再生許可時間が３０秒であれば、プレビューしただけでも最大１００円を課金することができることなる。

【０１１４】

さらに、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が有料であり、購入する場合には、例えば、予め、映像音声Ｍａｖ（暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））））を制作した制作者が設定した料金となる。或いは、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が有料であり、借用する（レンタルする）場合には、映像音声Ｍａｖ（暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））））を制作した制作者と暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を送信した放送局等の事業者との協議によって、一定期間何百円といったように設定したレンタル料となる。

【０１１５】

送出制御部４９は、ＥＣＭ－Ｋｃ解析部３５またはＥＣＭ－Ｋｗ解析部３７から出力されたスクランブル鍵Ｋｓを一時的に保持して、視聴プレビュー判定部４７から出力された制御情報に基づいて、当該スクランブル鍵Ｋｓをセキュリティモジュール２９の外部（デスクランブル部３１）への送出を制御するものである。

【０１１６】

ＶｉｅｗＬｏｇ課金部５１は、視聴プレビュー判定部４７から出力された課金情報に基づいて、通信回線網を介して徴収すべき料金を送信側に通知すると共に、視聴プレビュー判定部４７から出力された購入フラグ（購入フラグの数値）および再設定された有効期限を含めたコンテンツ利用制御情報と、再生時間カウント部４５でカウントした再生時間とを、映像音声Ｍａｖ（コンテンツ）毎に付されている識別情報であるコンテンツＩＤ毎に取りまとめたコンテンツ履歴情報を生成し、このコンテンツ履歴情報から購入フラグの値、有効期限のみを再暗号化Ｋｃ配布用ＥＣＭ解析部４１に出力するものである。このＶｉｅｗＬｏｇ課金部５１が特許請求の範囲の請求項に記載した課金手段に相当するものである。

【０１１７】

デスクランブル部３１は、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））をセキュリティモジュール２９の送出制御部４９から出力されたスクランブル鍵Ｋｓでデ

スクランブルして、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）を生成するものである。簡略に述べると、このデスクランブル部３１でデスクランブルしたＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）が暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の一部であれば、映像音声Ｍａｖの「プレビュー」といえることになる。

【０１１８】

ＭＰＥＧ２デコード部３３は、デスクランブル３１から出力されたＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）をデコードした映像音声Ｍａｖをコンテンツ受信装置２１の外部に備えられる表示装置（図示せず）に送出するものである。なお、デスクランブル部３１およびＭＰＥＧ２デコード部３３が特許請求の範囲の請求項に記載したコンテンツ復号出力手段に相当するものである。

【０１１９】

このコンテンツ受信装置２１によれば、受信分離部２３で、送信側のコンテンツ送信装置１から送信された多重暗号化コンテンツが受信されて、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））と、リアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））と、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とに分離される。コンテンツ蓄積部２５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））が蓄積される。

【０１２０】

そして、蓄積再生時に、Ｋｃ配布用ＥＣＭ解析部３９で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））がワーク鍵Ｋｗで復号化され、コンテンツ鍵Ｋｃおよびコンテンツ利用制御情報が取得される。ＥＣＭ－Ｋｃ解析部３５で、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））がコンテンツ鍵Ｋｃで復号化され、スクランブル鍵Ｋｓおよびコンテンツ経過時間情報が取得される。

【０１２１】

その後、視聴者の意向が参酌され、視聴プレビュー判定部４７でコンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて、映像音声Ｍａｖ（コンテンツ）をプレビューする（プレビュー可能か）または購入する若しくは借用する

（レンタルする）かどうかが判定され、判定結果により、コンテンツ利用制御情報の有効期限および購入フラグが再設定され、制御情報（スクランブル鍵Ｋｓの送出数に該当）が出力され、デスクランブル部３１およびＭＰＥＧ２デコード部３３で暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が映像音声Ｍａｖ（コンテンツ、またはコンテンツのプレビュー）として出力される。このため、蓄積再生時に、プレビューを視聴することができ、また、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて、プレビュー再生時間を制御することができ、より細かくプレビュー制御できる。

【０１２２】

また、このコンテンツ受信装置２１によれば、再生時間カウンタ部４５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））をスクランブル鍵Ｋｓで復号化して再生した再生時間がカウントされる。ＶｉｅｗＬｏｇ課金部５１で、コンテンツ利用制御情報に設定されている購入フラグが管理され、当該購入フラグにより暗号化コンテンツが有料である場合、再生時間カウンタ部４５でカウントされた再生時間に応じて課金される。ただし、視聴プレビュー判定部４７で、再生時間とコンテンツ利用制御情報に含まれる予め指定されたプレビュー再生許可時間とが比較判定された判定結果に基づき、再生時間がプレビュー再生許可時間を経過するまでは、ＶｉｅｗＬｏｇ課金部５１で課金されない。つまり、再生時間がプレビュー再生許可時間未満ではプレビューしているものとみなされ、課金されない。また任意に、課金することもできる。

【０１２３】

或いは、このコンテンツ受信装置２１によれば、記憶した情報が外部より読みとり不可能なセキュリティモジュール２９が備えられており、このセキュリティモジュール２９の内部で視聴プレビュー判定部４７による再生時間とプレビュー再生許可時間との比較判定が行われているので、再生時間と、プレビュー再生許可時間との双方が改ざんされるおそれがなく、比較判定を実行することができる。

【０１２４】

また、このコンテンツ受信装置２１によれば、セキュリティモジュール２９の

内部で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が扱われる場合、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））を識別する識別子であるコンテンツＩＤ毎に、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））に含まれているコンテンツ利用制御情報が整理され、再生時間カウンタ部４５でカウントされた再生時間が含められ、コンテンツ履歴情報とされる。このため、映像音声Ｍａｖ（コンテンツ）を提供したコンテンツ制作者や放送事業者等が、セキュリティモジュール２９からコンテンツ履歴情報を出力させる（吸い上げる）ことで、当該コンテンツ履歴情報によって、映像音声Ｍａｖ（コンテンツ）の利用状況を把握することができる。

【０１２５】

さらに、コンテンツ受信装置２１によれば、視聴プレビュー判定部４７で再生時間とプレビュー再生許可時間との比較判定した判定結果、再生時間がプレビュー再生許可時間に達していない場合、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１でコンテンツ履歴情報およびコンテンツＫｃを含む関連情報がセキュリティモジュール２９の内部に備えられる固有鍵で再暗号化された再暗号化Ｋｃ配布用ＥＣＭとされ、コンテンツ蓄積部２５に記憶される。このため、セキュリティモジュール２９の外部にあるコンテンツ蓄積部２５に、コンテンツ履歴情報およびコンテンツ鍵Ｋｃ等を出力して記憶しても、改ざんされるおそれがなく、当該コンテンツ履歴情報およびコンテンツ鍵Ｋｃを安全に保持することができる。なお、セキュリティモジュール２９内部にコンテンツ履歴情報およびコンテンツ鍵Ｋｃを記憶させることができるレジスト機構（メモリー：不揮発性メモリデバイス）を備えることで、これらコンテンツ履歴情報およびコンテンツ鍵Ｋｃを安全に保持することもできる。

【０１２６】

さらにまた、コンテンツ受信装置２１によれば、多重暗号化コンテンツを受信分離部２３で受信する度に、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））がセキュリティモジュール２９内部で復号化され、Ｋｃ配布用ＥＣＭが得られ、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））と共に、コンテンツ蓄積部２５に記憶される際に、再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１で再暗号化され、再

暗号化Ｋｃ配布用ＥＣＭとしてコンテンツ蓄積部２５に記憶される。これにより、セキュリティモジュール２９の外部にあるコンテンツ蓄積部２５に、Ｋｃ配布用ＥＣＭを出力して記憶しても、改ざんされるおそれがなく、当該Ｋｃ配布用ＥＣＭを安全に保持することができる。

【０１２７】

また、コンテンツ受信装置２１のＶｉｅｗＬｏｇ課金部５１で有料コンテンツを購入するか借用するかに関する情報（購入フラグの値）が、通信回線網を介して、コンテンツ送信装置１に通知されるので、コンテンツ送信装置１を使用する放送事業者は、有料コンテンツにかかる料金を確認することができる。

【０１２８】

また、コンテンツ受信装置２１の受信分離部２３で受信した多重暗号化コンテンツに第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が多重化されていない場合、Ｋｃ配布用ＥＣＭ解析部３９に備えられている第二暗号鍵関連情報要求手段で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が通信回線網を介してコンテンツ送信装置１に要求される。なおかつ、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が有料コンテンツである場合、ＶｉｅｗＬｏｇ課金部５１で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が取得される際に、有料コンテンツにかかる料金が課金される。つまり、このＶｉｅｗＬｏｇ課金部５１は、Ｋｃ配布課金方式（コンテンツ鍵Ｋｃを受領した時点で課金される方式）を兼ね備えており、これにより、コンテンツ受信装置２１では、ＶｉｅｗＬｏｇ課金方式（実際に視聴した時間（再生時間）に基づいて課金される方式）とＫｃ配布課金方式との双方の運用を実現することができる。

【０１２９】

（コンテンツ送信装置の動作）

次に、図３に示すフローチャートを参照して、コンテンツ送信装置１の動作を説明する（適宜、図１参照）。

まず、映像音声Ｍａｖ（コンテンツ）がコンテンツ送信装置１のＭＰＥＧ２エンコード部３に入力され、このＭＰＥＧ２エンコード部３で映像音声Ｍａｖ（コンテンツ）がエンコードされて、ＭＰＥＧ２形式の映像音声コンテンツストリー

ム（ＴＳ）とされスクランブル部５へ出力される（Ｓ１）。

【０１３０】

続いて、スクランブル部５で映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵Ｋｓでスクランブルされて、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））とされ、多重化部１５へ出力される（Ｓ２）。このスクランブル部５で使用されたスクランブル鍵Ｋｓに当該スクランブル鍵Ｋｓに関する情報が付加されて、スクランブル鍵Ｋｓを含む関連情報とされ、このスクランブル鍵Ｋｓを含む関連情報がＥＣＭ－Ｋｗ生成部７およびＥＣＭ－Ｋｃ生成部１１に入力される。また、現在時刻情報がＥＣＭ－Ｋｗ生成部７に入力される。

【０１３１】

すると、ＥＣＭ－Ｋｗ生成部７で、スクランブル鍵Ｋｓを含む関連情報および現在時刻情報がワーク鍵Ｋｗで暗号化されて、受信再生時第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））とされ、多重化部１５へ出力される（Ｓ３）。

【０１３２】

また、コンテンツ送出管理部９からコンテンツ経過時間情報および連続指標がＥＣＭ－Ｋｃ生成部１１に出力され、コンテンツ送出情報が多重化部１５に出力される（Ｓ４）。ＥＣＭ－Ｋｃ生成部１１で、スクランブル鍵Ｋｓを含む関連情報、コンテンツ経過時間情報および連続指標がコンテンツ鍵Ｋｃで暗号化されて、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））とされ、多重化部１５へ出力される（Ｓ５）。このＥＣＭ－Ｋｃ生成部１１で使用されたコンテンツ鍵Ｋｃに当該コンテンツ鍵Ｋｃに関する情報が付加されて、コンテンツ鍵Ｋｃを含む関連情報とされ、このコンテンツ鍵Ｋｃを含む関連情報がＫｃ配布用ＥＣＭ生成部１３に入力される。また、コンテンツ経過時間情報がＥＣＭ－Ｋｃ生成部１１に入力される。

【０１３３】

すると、Ｋｃ配布用ＥＣＭ生成部１３で、コンテンツ鍵Ｋｃを含む関連情報およびコンテンツ利用制御情報がワーク鍵Ｋｗで暗号化されて、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））とされ、多重化部１５へ出力される（Ｓ６）。その後、多重化部１５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））、リア

ルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））、コンテンツ送出情報および第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））が多重化されて、多重暗号化コンテンツとされ、送出される（Ｓ７）。

【０１３４】

（コンテンツ受信装置の動作）

次に、図４、図５に示すフローチャートを参照して、コンテンツ受信装置２１の動作を説明する（適宜、図２参照）。なお、このコンテンツ受信装置２１の動作の説明では、送信側のコンテンツ送信装置１から送信された多重暗号化コンテンツを受信した後、再生するまでの概略を説明したもので、当該コンテンツ受信装置２１の主要部分である視聴プレビュー判定部４７の動作は、図６に示すフローチャートを参照して説明する。また、このコンテンツ受信装置２１の動作の説明では、多重暗号化コンテンツを復号化またはデスクランブルにかかる情報のみに言及して説明している。

【０１３５】

送信側のコンテンツ送信装置１から送出された多重暗号化コンテンツが、コンテンツ受信装置２１の受信分離部２３で受信される（Ｓ１１）。そして、コンテンツ受信装置２１の使用者（視聴者）は、リアルタイムに受信しながら映像音声Ｍａｖ（コンテンツ）を視聴する（再生する）か、一旦、コンテンツ蓄積部２５に蓄積後、後ほど、映像音声Ｍａｖ（コンテンツ）を視聴する（再生する）かを決定し、つまり、受信再生するか（リアルタイム受信再生）蓄積再生するか（蓄積再生）を決定する。

【０１３６】

このコンテンツ受信装置２１の使用者（視聴者）の意向に基づいて、コンテンツ受信装置２１に備えられている操作部（図示せず）の再生ボタンが押下されると、コンテンツ受信装置２１では、当該装置２１の主制御部（図示せず）によって、リアルタイム受信再生するかどうかが判断される（Ｓ１２）。リアルタイム受信再生すると判断された場合（Ｓ１２、Ｙｅｓ）、受信分離部２３で多重暗号化コンテンツが分離され、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がコンテン

ツ蓄積部２５に出力され蓄積された後、間髪をおかずに（ほぼ同時に）暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））が分離部２７に、リアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））がセキュリティモジュール２９のＥＣＭ－Ｋｗ解析部３７に出力される（Ｓ１３）。

【０１３７】

すると、まず、分離部２７で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がデスクランブル部３１に出力され（Ｓ１４）、続いて、ＥＣＭ－Ｋｗ解析部３７でリアルタイム受信時用第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｗ，Ｋｗ））がワーク鍵Ｋｗで復号化され、スクランブル鍵Ｋｓおよび現在時刻情報が取得され、スクランブル鍵Ｋｓが送出制御部４９に、現在時刻情報が視聴プレビュー判定部４７に出力される（Ｓ１５）。

【０１３８】

また、Ｓ１２にて、リアルタイム受信再生すると判断されない場合（Ｓ１２、Ｎｏ）、つまり、蓄積再生される場合には、受信分離部２３で、多重暗号化コンテンツが、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））および第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ）
に分離され、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））がコンテンツ蓄積部２５に、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））がセキュリティモジュール２９のＫｃ配布用ＥＣＭ解析部３９に出力される（Ｓ１６）。

【０１３９】

コンテンツ蓄積部２５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））が蓄積され、コンテンツ受信装置２１の使用者（視聴者）に意向により、操作部（図示せず）の再生ボタンが押下されるまで待機される。その後、当該再生ボタンが押下された場合（蓄積再生時）に、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））が分離部２７に出力される（Ｓ１７）。すると、分離部２７で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））および第一暗号鍵関連情

報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））が分離され、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がデスクランブル部３１に、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））がセキュリティモジュール２９のＥＣＭ－Ｋｃ解析部３５に出力される（Ｓ１８）。

【０１４０】

すると、まず、Ｋｃ配布用ＥＣＭ解析部３９で、第二暗号鍵関連情報（Ｅ（Ｋｃ配布用ＥＣＭ，Ｋｗ））がワーク鍵Ｋｗで復号化され、コンテンツ鍵ＫｃおよびコンテンツＫｃがＥＣＭ－Ｋｃ解析部３５に、コンテンツ利用制御情報が視聴プレビュー判定部４７に出力される（Ｓ１９）。続いて、ＥＣＭ－Ｋｃ解析部３５で、第一暗号鍵関連情報（Ｅ（ＥＣＭ－Ｋｃ，Ｋｃ））がコンテンツ鍵Ｋｃで復号化され、スクランブル鍵Ｋｓ、コンテンツ経過時間情報および連続指標が取得され、スクランブル鍵Ｋｓが送出制御部４９に、コンテンツ経過時間情報が視聴プレビュー判定部４７に、連続指標が再生時間カウンタ部４５に出力される（Ｓ２０）。ここから図５を参照して説明を続ける。

【０１４１】

視聴プレビュー判定部４７で、視聴プレビューが判定され（視聴可能判定）、制御情報が送出制御部４９に、課金情報、購入フラグの値および有効期限がＶｉｅｗＬｏｇ課金部５１に出力される（Ｓ２１）。送出制御部４９で制御情報に基づいて、デスクランブル部３１に出力されるスクランブル鍵Ｋｓが制御される（Ｓ２２）。デスクランブル部３１にスクランブル鍵Ｋｓが入力されると、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））がデスクランブルされ、ＭＰＥＧ２形式の映像音声Ｍａｖコンテンツストリーム（ＴＳ）が得られ、ＭＰＥＧ２デコード部３３に出力される（Ｓ２３）。ＭＰＥＧ２デコード部３３で、ＭＰＥＧ２形式の映像音声Ｍａｖコンテンツストリーム（ＴＳ）がデコードされ映像音声Ｍａｖ（コンテンツ）が出力される（Ｓ２４）。

【０１４２】

また、視聴プレビュー判定部４７で出力された課金情報、購入フラグの値および有効期限がＶｉｅｗＬｏｇ課金部５１に入力されると、このＶｉｅｗＬｏｇ課

金部５１で、課金情報、購入フラグの値が通信回線網を介して送信側に送出されると共に、当該購入フラグの値、有効期限が再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１に出力される（Ｓ２５）。この課金情報に基づいて、図示を省略した表示部に徴収料金が表示される。

【０１４３】

さらにまた、Ｋｃ配布用ＥＣＭ解析部３９で復号化されたＫｃ配布用ＥＣＭが再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１に入力される。この再暗号化Ｋｃ配布用ＥＣＭ生成解析部４１で、Ｋｃ配布用ＥＣＭに含まれているコンテンツ利用制御情報に再生時間カウンタ部４５でカウントした再生時間が付加されたコンテンツ履歴情報と、ＶｉｅｗＬｏｇ課金部５１から入力された購入フラグの値および有効期限とが固有鍵で暗号化されて、再暗号化Ｋｃ配布用ＥＣＭとされ、コンテンツ蓄積部２５に出力される（Ｓ２６）。

【０１４４】

そして、コンテンツ蓄積部２５で、再暗号化Ｋｃ配布用ＥＣＭと暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））とが関係づけられて記憶される（Ｓ２７）。

次に、図６を参照して、視聴プレビュー判定部４７の動作を主に、コンテンツをプレビューして購入または借用（レンタル）する場合について説明する。

【０１４５】

視聴プレビュー判定部４７では、まず、コンテンツ利用制御情報に規定されている購入フラグが無料コンテンツを示すものかどうかが判断される（Ｓ３１）。購入フラグが無料コンテンツを示すものであると判定された場合（Ｓ３１、Ｙｅｓ）、この視聴プレビュー判定部４７から送出制御部４９に、全スクランブル鍵Ｋｓ送出可を示す制御信号が出力され、課金情報（０円）がＶｉｅＬｏｇ課金部５１に出力される（Ｓ３４）。また、Ｓ３１にて、購入フラグが無料コンテンツを示すものであると判定されない場合（Ｓ３１、Ｎｏ）は、有料コンテンツということになり、まず、購入フラグが購入済みを示すものかどうかが判定される（Ｓ３２）。

【０１４６】

購入フラグが購入済みを示すものである場合（Ｓ３２、Ｙｅｓ）、コンテンツ

利用制御情報の有効期限が無期限に再設定される（Ｓ３３）。この視聴プレビュー判定部４７から送出制御部４９に、全スクランブル鍵Ｋｓ送出可を示す制御情報が出力され、課金情報（コンテンツの料金）がＶｉｅＬｏｇ課金部５１に出力される（Ｓ３４）。

【０１４７】

Ｓ３２にて、購入フラグが購入済みを示すものでない場合（Ｓ３２、Ｎｏ）、コンテンツ受信装置２１の使用者（視聴者）に対して、図示を省略した表示部にプレビューするか否かの判断を催促するメッセージ（プレビュー視聴するか？）が表示される（Ｓ３５）。コンテンツ受信装置２１の使用者（視聴者）がプレビューを視聴しないと判断した場合には、コンテンツ受信装置２１の操作部（図示せず）のプレビュー取消ボタンが押下され（Ｓ３５、Ｎｏ）、当該ボタンが押下されることによって生じる制御信号によって、コンテンツ受信装置２１の視聴プレビュー判定部４７はプレビューすることなく動作を終了させる。

【０１４８】

Ｓ３５にて、コンテンツ受信装置２１の使用者（視聴者）がプレビューを視聴すると判断した場合には、コンテンツ受信装置２１の操作部（図示せず）のプレビュー実行ボタンが押下され（Ｓ３５、Ｙｅｓ）、当該ボタンが押下されることによって生じる制御信号によって、コンテンツ受信装置２１の視聴プレビュー判定部４７は、現在の時刻（プレビュー可能箇所）が、コンテンツ利用制御情報のプレビュー開始時刻・終了時刻（プレビュー許可期間）内であるかどうかを判定する（Ｓ３６）。現在の時刻（プレビュー可能箇所）が、プレビュー開始時刻・終了時刻（プレビュー許可期間）内であると判定された場合（Ｓ３６、Ｙｅｓ）、再生時間カウンタ部４５から再生時間を取得する（Ｓ３７）。

【０１４９】

再生時間カウンタ部４５から取得された再生時間がコンテンツ利用制御情報に含まれるプレビュー再生許可時間内であるかどうかが判定される（Ｓ３８）。再生時間がプレビュー再生許可時間内であると判定された場合（Ｓ３８、Ｙｅｓ）には、プレビュー可と判定され、一部のスクランブル鍵Ｋｓ送出可を示す制御情報が出力され、課金情報（０円またはプレビュー時間分に応じた料金）がＶｉｅ

Ｌｏｇ課金部５１に出力される（Ｓ３９）。

【０１５０】

コンテンツ受信装置２１の使用者（視聴者）がプレビューを視聴した後、コンテンツ受信装置２１の操作部（図示せず）の購入確認ボタンが押下された場合（Ｓ４０、Ｙｅｓ）、当該ボタンが押下されることによって生じる制御信号によって、コンテンツ受信装置２１の視聴プレビュー判定部４７は、購入フラグの値を、購入済みを示すものに再設定すると共に、コンテンツ利用制御情報の有効期限を無期限に再設定し（Ｓ４１）、この視聴プレビュー判定部４７から送出制御部４９に、全スクランブル鍵Ｋｓ送出可を示す制御情報が出力され、課金情報（コンテンツの料金）がＶｉｅＬｏｇ課金部５１に出力される（Ｓ３４）。

【０１５１】

また、コンテンツ受信装置２１の使用者（視聴者）がプレビューを視聴した後、コンテンツ受信装置２１の操作部（図示せず）の購入確認ボタンが押下されず（Ｓ４０、Ｎｏ）、借用確認ボタンが押下された場合（Ｓ４２、Ｙｅｓ）、当該ボタンが押下されることによって生じる制御信号によって、コンテンツ受信装置２１の視聴プレビュー判定部４７は、購入フラグの値を、借用を示すものに再設定すると共に、コンテンツ利用制御情報の有効期限を有限（任意の借用期間）に再設定し（Ｓ４３）、この視聴プレビュー判定部４７から送出制御部４９に、全スクランブル鍵Ｋｓ送出可を示す制御情報が出力され、課金情報（借用期間に応じた料金）がＶｉｅＬｏｇ課金部５１に出力される（Ｓ３４）。

【０１５２】

なお、プレビュー許可期間内であると判定されない場合（Ｓ３６、Ｎｏ）、再生時間がプレビュー再生許可時間内でないと判定された場合（Ｓ３８、Ｎｏ）には視聴プレビュー判定部４７はプレビューさせることなく動作を終了させる。また、購入確認ボタンと借用確認ボタンとの両方のボタンが押下されない場合（Ｓ４２、Ｎｏ）には、プレビューした再生時間が再生時間カウンタ部４５でカウントされるのみで、視聴プレビュー判定部４７は動作を終了させる。

【０１５３】

（コンテンツ経過時間情報について）

次に、図７を参照して、コンテンツ経過時間情報について説明する。

この図７は、図式的（概念的）に表現した１時間番組であるコンテンツに対し、コンテンツ経過時間の付与の仕方を例示したもので、図７（Ａ）は通常再生時間（実際の再生時間）と等しいコンテンツ経過時間を付与した場合を示したものであり、図７（Ｂ）は通常再生時間とは異なる時間経過で、コンテンツ経過時間を付与した場合を示したものであり、図７（Ｃ）は通常再生時間とは異なる時間経過でコンテンツ経過時間を付与した場合（減少する場合）を示したものである。

【０１５４】

図７（Ａ）に示したコンテンツ経過時間情報は、実際の再生時間と同様にコンテンツ経過時間が付与されてなるものであり、これによれば、コンテンツ経過時間情報が、コンテンツの開始時刻から連続して再生した場合の経過時間に対応する値であるので、コンテンツ受信装置２１で、当該コンテンツをプレビューさせる場合に、単純に、コンテンツの経過時間に対応するプレビューを生成できる。

【０１５５】

図７（Ｂ）に示したコンテンツ経過時間情報は、実際の再生時間とは異なった時間軸上の経過時間が付与されてなるものであり、この図中に示したように、コンテンツの内容に応じて、経過時間が異なっており、重要でないシーンは粗く、重要なシーンは細かく、不均一に経過時間が付与されている。これによれば、コンテンツ受信装置２１で、当該コンテンツをプレビューさせる場合に、送信側の意図（放送局等のコンテンツを制作した制作者の意図）に合わせたコンテンツのプレビューの制御が容易に実現される。

【０１５６】

図７（Ｃ）に示したコンテンツ経過時間情報は、実際の再生時間とは異なった時間軸上の経過時間が付与されてなるものであり、この図中に示したように、コンテンツ内容に直接関係のない（重要でない）プロモーションやＣＭ等の部分における経過時間が、経過すると共に減少するように付与されている。これによれば、プロモーションやＣＭ等を視聴することで、結果的に、コンテンツのプレビュー再生時間を多くさせることができ、プロモーションやＣＭ等を視聴した視聴

者に対しサービスを提供したことになり、サービスを提供された視聴者の購買意欲を刺激することができる。

【０１５７】

また、例えば、コンテンツのハイライトの部分では、短時間でプレビューの時間が終了してしまうように送信側で設定しておけば、コンテンツ受信装置２１の使用者（視聴者）は、コンテンツの全体を視聴したいとの欲求が高まり、この結果、コンテンツの購買意欲を増進させることができる。

【０１５８】

（再生時間カウンタ部の演算方式について）

次に、図８を参照して、再生時間カウンタ部４５の演算方式、つまり、プレビュー再生時間の計測の仕方について説明する。図８は、再生時間カウンタ部４５の演算方式を模式的に表現した説明図であり、図８（ａ）は連続指標がない場合の再生時間カウンタ部４５の演算方式を示したものであり、図８（ｂ）は連続指標がない場合であり、かつ、一定の基準で正確な再生時間をカウントできるように工夫した場合の再生時間カウンタ部４５の演算方式を示したものであり、図８（ｃ）は連続指標がある場合の再生時間カウンタ部４５の演算方式を示したものである。

【０１５９】

図８に示したように、いずれの演算方式も、隣接するＥＣＭ－Ｋｃ内の経過時間（１つ前に受けたＥＣＭ－Ｋｃ内の経過時間と、現在のＥＣＭ－Ｋｃ内の経過時間とによる時間）に基づいて、再生時間を演算するものである。図８（ａ）に示した演算方式は、１つ前に受けたＥＣＭ－Ｋｃ内の経過時間と現在のＥＣＭ－Ｋｃ内の経過時間とによる時間との差分を演算し、演算結果の総和を再生時間としてカウントするものである。

【０１６０】

図８（ｂ）に示した演算方式は、１つ前に受けたＥＣＭ－Ｋｃ内の経過時間と現在のＥＣＭ－Ｋｃ内の経過時間とによる時間との差分を演算し、この差分がある値Ａ（例えば、Ａ＝３秒）よりも大きければ０とみなし、Ａ以下であれば、演算結果に反映させて（加算する）、演算結果の総和を再生時間としてカウントす

るものである。なお、ある値Ａは、スクランブル鍵Ｋｓの変更単位時間と同じ値をとるものでよい。

【０１６１】

図８（ｃ）に示した演算方式は、連続時間を連続指標に基づいてチェックし、連続していれば、１つ前に受けたＥＣＭ－Ｋｃ内の経過時間と現在のＥＣＭ－Ｋｃ内の経過時間とによる時間との差分を演算し、不連続であれば、０として演算結果の総和を再生時間としてカウントするものである。

【０１６２】

すなわち、コンテンツ受信装置２１で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の特定部分をプレビューした場合、このプレビューがリニア再生であれば、再生時間カウンタ部４５で、実際の経過時間を再生時間としてカウントすることができる。ところが、プレビューをノンリニア再生させる場合では、実際の経過時間と、再生時間とが異なる場合が生じる。この差異を補完するために、コンテンツ受信装置２１では、連続指標を用いている。

【０１６３】

これによれば、再生時間カウンタ部４５で、暗号化コンテンツ（Ｅ（Ｍａｖ，Ｋｓ））の特定部分をプレビューとしてノンリニア再生した再生時間が、連続指標に基づいて、正確にカウントすることができる。

【０１６４】

（コンテンツ利用制御情報とコンテンツの履歴情報とについて）

次に、図９を参照して、コンテンツ利用制御情報とコンテンツの履歴情報とについて説明する。図９（ａ）はコンテンツ利用制御情報を示したものであり、図９（ｂ）はコンテンツ履歴情報を示したものである。

【０１６５】

図９（ａ）に示したように、コンテンツ利用制御情報には、有効期限「０２／０８／０６　２４：００：００」と、プレビュー開始時刻「００：００：００」と、プレビュー終了時刻「００：００：１５」と、プレビュー再生許可時間「００：００：２０」と、購入フラグ「ＰＦ」とが含まれている。

【０１６６】

有効期限「０２／０８／０６　２４：００：００」は、コンテンツが利用できる期限が２００２年の８月６日２４時までであることを示しており、プレビュー開始時刻「００：００：００」は、プレビューを開始する時刻がコンテンツの開始から０秒（初めから）であることを示しており、プレビュー終了時刻「００：００：１５」は、プレビューを終了する時刻がコンテンツの開始から１５秒であることを示している。

【０１６７】

また、プレビュー再生許可時間「００：００：２０」は、プレビューできる再生時間の最大が２０秒であることを示しており、購入フラグ「ＰＦ」は、コンテンツが“ＰａｙＦｒｅｅ”、つまり、無料であることを示している。なお、このＰＦが「購入フラグの数値」にあたるものである。通常、購入フラグの数値は整数で表現され、例えば「０」が有料で未購入、「１」が有料で購入済み、「２」が有料でレンタル中、「３」が無料と設定することができる。

【０１６８】

図９（ｂ）に示したように、コンテンツ履歴情報は、コンテンツ利用制御情報に、コンテンツＩＤ、コンテンツ鍵Ｋｃ、再生時間を含んで構成されるものである。つまり、このコンテンツ履歴情報を用いれば、コンテンツ状況を一括して管理することができる。なお、この実施の形態では、このコンテンツ履歴情報は、セキュリティモジュール２９のＶｉｅｗＬｏｇ課金部５１で管理されている。

【０１６９】

（プレビュー用コンテンツが予め付加されているコンテンツについて）

次に、図１０を参照して、プレビュー用コンテンツが予め付加されているコンテンツについて、従来のコンテンツと比較しながら説明する。

【０１７０】

図１０（ａ）は、従来のコンテンツにおけるプレビューを示したものであり、図１０（ｂ）は、プレビュー用コンテンツが予め付加されているコンテンツを示したものである。この図１０（ａ）に示すように、従来のコンテンツにおけるプレビューでは、プレビュー開始時刻からプレビュー終了時刻までのコンテンツの冒頭部分しか、受信側の視聴者は試視聴することができなかったが、図１０（ｂ

）に示すように、コンテンツの先頭に、予め、当該コンテンツの任意の部分を取り出して編集制作したプレビュー用コンテンツを付加されている。

【０１７１】

そして、このプレビュー用コンテンツの利用制御が、コンテンツ受信装置２１により、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて行われる。このため、送信者側の意図に応じて、編集または制作したプレビューを取り扱うことができ、受信側の視聴者に、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいてプレビュー用コンテンツを視聴させることができる。

【０１７２】

以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。

例えば、コンテンツ送信装置１およびコンテンツ受信装置２１の各構成の処理を一つずつの過程ととらえ、コンテンツ送信方法およびコンテンツ受信方法とみなすことや、コンテンツ送信装置１およびコンテンツ受信装置２１の各構成の処理を汎用のコンピュータ言語で記述したコンテンツ送信プログラムおよびコンテンツ受信プログラムとみなすこともできる。

【０１７３】

こういった場合、コンテンツ送信装置１およびコンテンツ受信装置２１と同様の効果を得ることができる。また、コンテンツ送信プログラムおよびコンテンツ受信プログラムとした場合には、これらのプログラムを記録媒体等に記録して流通させることもできる。

【０１７４】

【発明の効果】

請求項１、２、９記載の発明によれば、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。第一鍵を含む関連情報およびコンテンツの経過時間に関する情報であるコンテンツ経過時間情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。第二暗号鍵を含む関連情報および受信側におけるコンテンツの利用を制御する情報であるコンテンツ利用制御情報が第三暗号鍵で暗号化され、第二暗号鍵関連情報とされる。その後、暗号化コンテンツと、第一暗号

鍵関連情報と、第二暗号化鍵関連情報とが多重化されて多重暗号化コンテンツとして出力される。このため、例えば、受信側で、この多重暗号化コンテンツが受信されれば、コンテンツ経過時間情報に基づいて、多重暗号化コンテンツの一部が通常の視聴形態に対して異なる視聴形態に生成でき、コンテンツ利用制御情報に基づいて、再生時間が制御された視聴形態により視聴することができる。

【０１７５】

請求項３記載の発明によれば、コンテンツ経過時間情報において、経過時間が、コンテンツの開始時刻から連続して再生した場合の再生時間に対応する値であるので、プレビュー機能を備えた装置を有する受信側では、単純に、コンテンツの経過時間に対応して異なる視聴形態に生成できる。

【０１７６】

請求項４記載の発明によれば、コンテンツ経過時間情報において、経過時間が、コンテンツの開始時刻から連続して再生した場合の再生時間とは異なる不均一な値であり、つまり、コンテンツ経過時間情報が実際の再生時間によるものではなく、コンテンツの内容に応じて（即して）、異なる値に指定されている。このため、受信側では、送信側の意図に応じた（コンテンツの内容に即した）コンテンツの異なる視聴形態による視聴を実現することができる。

【０１７７】

請求項５記載の発明によれば、コンテンツ経過時間情報において、経過時間が、コンテンツの各時点での内容に応じて（即して）、コンテンツの開始時刻から連続して再生した場合の再生時間に対して増減した値であり、つまり、コンテンツ経過時間情報が実際の再生時間によるものではなく、コンテンツの各時点での内容に応じて、増減した値に指定される。このため、例えば、コンテンツのハイライトの部分では、短時間でプレビューの時間が終了してしまうように送信側で設定しておけば、プレビュー機能を備えた装置を有する受信側の視聴者は、コンテンツの全体を視聴したいとの欲求が高まり、この結果、コンテンツの購買意欲を増進させることができる。

【０１７８】

請求項６記載の発明によれば、コンテンツの先頭に、当該コンテンツの任意の

部分を取り出したプレビュー用コンテンツが配置されているので、プレビュー機能を備えた装置を有する受信側の視聴者に、送信者側の意図に応じたプレビュー用コンテンツを視聴させることができる。

【０１７９】

請求項７記載の発明によれば、コンテンツが有料コンテンツである場合、当該有料コンテンツを購入または借用したかどうかを判定する購入フラグがコンテンツ利用制御情報内に設定される。そして、プレビュー機能を備えた装置を有する受信側で有料コンテンツが購入された場合または借用された場合には購入フラグの値が変更され返信されれば、これにより、受信側で、有料コンテンツの徴収料金を確認することができる。

【０１８０】

請求項８記載の発明によれば、第二暗号鍵関連情報が暗号化コンテンツとは別に送信されるので、受信者側で、暗号化コンテンツを復号化してコンテンツを視聴したい場合に、送信側に要求が出され、この要求に基づいて第二暗号鍵関連情報が出力される。これによって、送信側では、受信側でコンテンツを視聴したとみなして、的確な課金をすることができる。

【０１８１】

請求項１０、１１、２０記載の発明によれば、多重暗号化コンテンツが受信され、当該多重暗号化コンテンツに多重化されている暗号化コンテンツ、第一暗号鍵関連情報および第二暗号鍵関連情報が分離される。暗号化コンテンツおよび第一暗号鍵関連情報が蓄積された後、第二暗号鍵関連情報が第三暗号鍵で復号化され、コンテンツ利用制御情報および第二暗号鍵が取得され、第一暗号鍵関連情報が第二暗号鍵で復号化され、コンテンツ経過時間情報および第一暗号鍵が取得される。その後、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて、暗号化コンテンツの特定部分を視聴可能か判定され、判定結果に基づいて、暗号化コンテンツの特定部分が第一暗号鍵で復号化されて異なる視聴形態に出力される。このため、蓄積再生時に、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて、異なる視聴形態による視聴をすることができ（生成でき）、また、コンテンツ経過時間情報およびコンテンツ利用制御情報に基づいて、

異なる視聴形態による再生時間を制御することができ、例えば、異なる視聴形態として、コンテンツの特定部分をプレビューする場合、このプレビューをより細かくプレビュー制御できる。

【０１８２】

請求項１２記載の発明によれば、暗号化コンテンツを第一暗号鍵で復号化して再生した再生時間がカウントされ、コンテンツ利用制御情報に設定されている購入フラグが管理され、当該購入フラグにより暗号化コンテンツが有料である場合、カウントされた再生時間に応じて課金することができる。

【０１８３】

請求項１３記載の発明によれば、第一暗号鍵関連情報に含まれている前記第一暗号鍵が変更される変更単位時間に対応して付される連続指標に基づいて、プレビューをノンリニア再生した場合であっても、再生時間を正確にカウントすることができる。

【０１８４】

請求項１４記載の発明によれば、セキュリティモジュールの内部で再生時間と再生許可時間との比較判定が行われるので、再生時間と、再生許可時間との双方が改ざんされるおそれがなく、比較判定を実行することができる。

【０１８５】

請求項１５記載の発明によれば、セキュリティモジュールの内部で、暗号化コンテンツを識別する識別子であるコンテンツＩＤ毎に、第二暗号鍵関連情報に含まれているコンテンツ利用制御情報が関連付けられ、カウントされた再生時間が含められ、コンテンツ履歴情報とされる。このため、コンテンツを提供したコンテンツ制作者や放送事業者等が、セキュリティモジュールからコンテンツ履歴情報を出力させる（吸い上げる）ことで、当該コンテンツ履歴情報によって、コンテンツの利用状況を把握することができる。

【０１８６】

請求項１６記載の発明によれば、再生時間が再生許可時間に達していない場合、コンテンツ履歴情報および第二暗号鍵を含む関連情報がセキュリティモジュールの内部に備えられる固有鍵で再暗号化され、暗号化コンテンツ蓄積手段に記憶

される。このため、セキュリティモジュールの外部にある暗号化コンテンツ蓄積手段に、コンテンツ履歴情報および第二暗号鍵等を出力して記憶しても、改ざんされるおそれがなく、当該コンテンツ履歴情報および第二暗号鍵等を安全に保持することができる。なお、セキュリティモジュール内部にコンテンツ履歴情報および第二暗号鍵を記憶させることができるレジスト機構（メモリー）が備えられていれば、このレジスト機能に記憶しておくことも可能である。

【０１８７】

請求項１７記載の発明によれば、多重暗号化コンテンツを受信する度に、第二暗号鍵関連情報がセキュリティモジュール内部で復号化され、暗号化コンテンツと共に、暗号化コンテンツ蓄積手段に記憶される際に、再暗号化手段で再暗号化される。これにより、セキュリティモジュールの外部にある暗号化コンテンツ蓄積手段に、第二暗号鍵関連情報を出力して記憶しても、改ざんされるおそれがなく、当該第二暗号鍵関連情報を安全に保持することができる。

【０１８８】

請求項１８記載の発明によれば、有料コンテンツを購入するか借用するかに関する情報が、通信回線網を介して、コンテンツ送信装置に通知される。これにより、コンテンツ送信装置を有するコンテンツ提供者（放送局等の事業者）は、有料コンテンツにかかる料金を確認することができる。

【０１８９】

請求項１９記載の発明によれば、受信した多重暗号化コンテンツに第二暗号鍵関連情報が多重化されていない場合、第二暗号鍵関連情報が通信回線網を介してコンテンツ送信装置に要求される。なおかつ、暗号化コンテンツが有料コンテンツである場合、第二暗号鍵関連情報（第二暗号鍵）が取得される際に、有料コンテンツにかかる料金が課金される。これにより、実際に視聴した時間に基づいて課金されるＶｉｅｗＬｏｇ課金方式と第二暗号鍵を取得した時点で課金されるＫｃ配布課金方式との双方の運用を実現することができる。

【図面の簡単な説明】

【図１】

本発明による一実施の形態であるコンテンツ送信装置のブロック図である。

【図２】

本発明による一実施の形態であるコンテンツ受信装置のブロック図である。

【図３】

図１に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図４】

図２に示したコンテンツ受信装置の動作を説明したフローチャートである。

【図５】

図２に示したコンテンツ受信装置の動作を説明したフローチャート（図４の続き）である。

【図６】

視聴プレビュー判定部の動作を説明したフローチャートである。

【図７】

コンテンツ経過時間情報を説明した図である。

【図８】

再生時間カウンタ部の演算方式を説明した図である。

【図９】

コンテンツ利用制御情報およびコンテンツ履歴情報を説明した図である。

【図１０】

プレビュー用コンテンツが予め付加されているコンテンツについて、従来のコンテンツと比較して説明した図である。

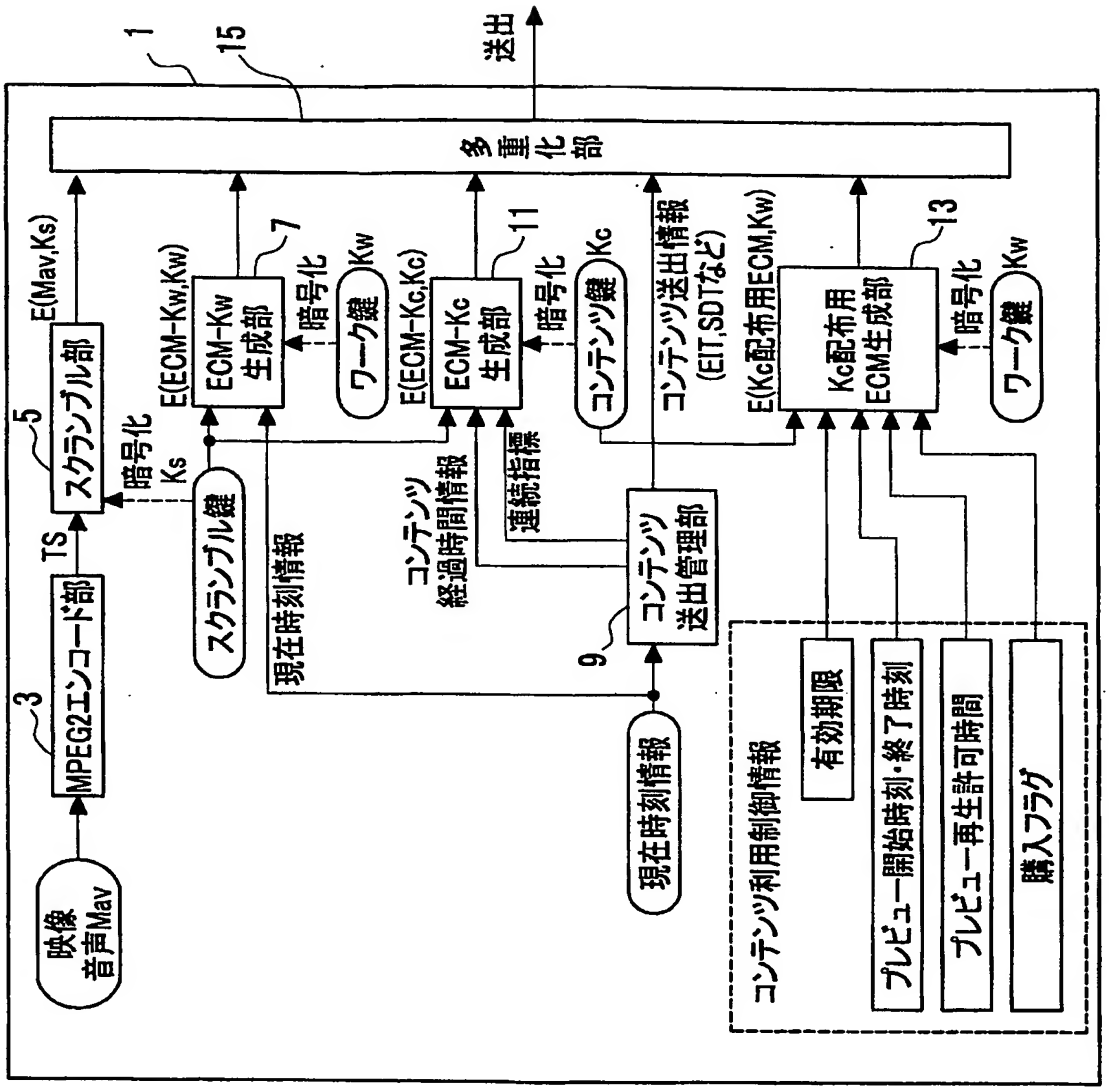
【符号の説明】

| | |
|---|---|
| １ | コンテンツ送信装置 |
| ３ | ＭＰＥＧ２エンコード部 |
| ５ | スクランブル部（コンテンツ暗号化手段） |
| ７ | ＥＣＭ－Ｋｗ生成部 |
| ９ | コンテンツ送出管理部（コンテンツ送出管理手段） |
| １１ | ＥＣＭ－Ｋｃ生成部（第一暗号鍵暗号化手段） |
| １３ | Ｋｃ配布用ＥＣＭ生成部（第二暗号鍵暗号化手段） |
| １５ | 多重化部（多重出力手段） |

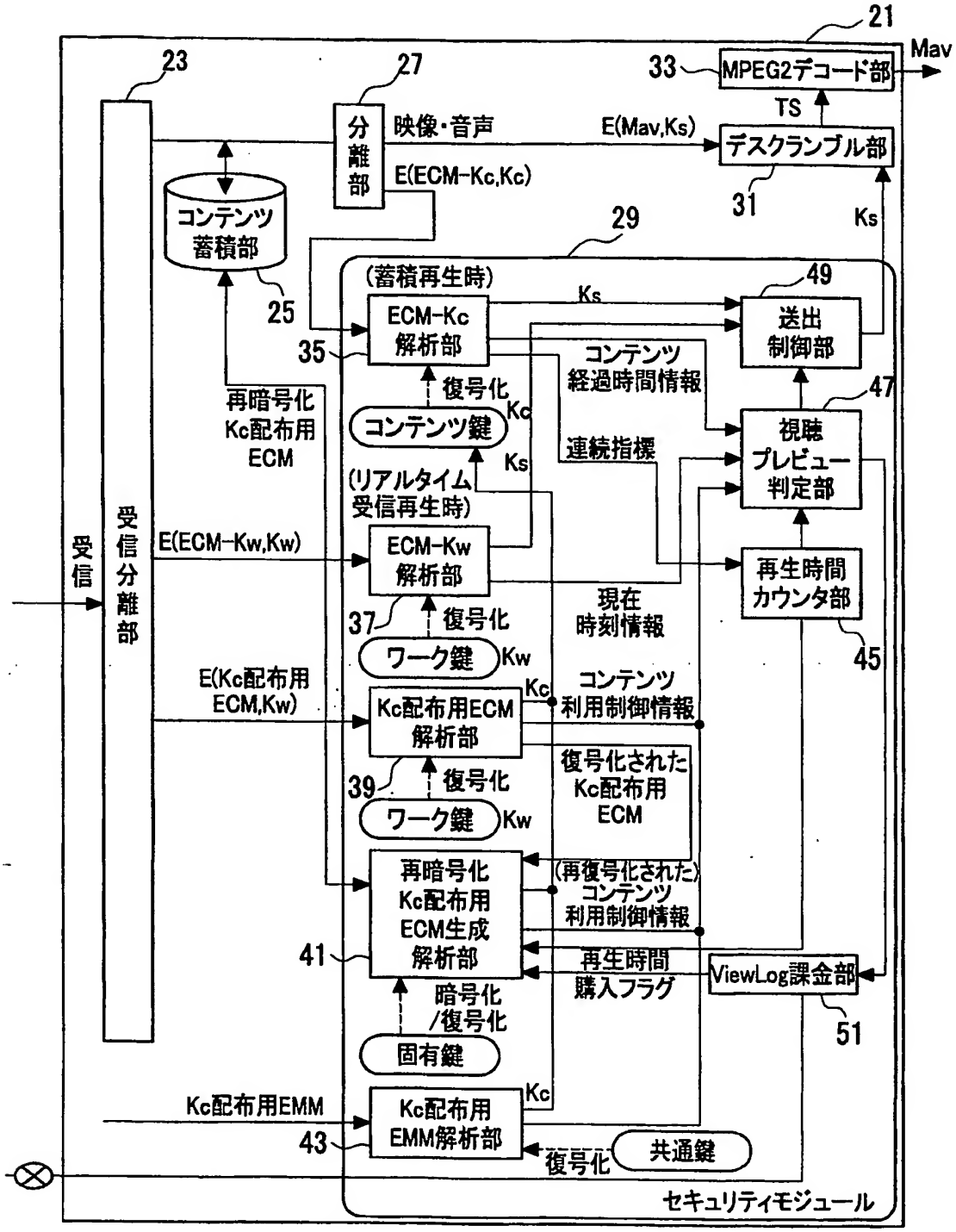
２１　　コンテンツ送信装置
２３　　受信分離部（受信分離手段）
２５　　コンテンツ蓄積部（暗号化コンテンツ蓄積手段）
２７　　分離部
２９　　セキュリティモジュール
３１　　デスクランブル部（コンテンツ復号化出力手段）
３３　　ＭＰＥＧ２デコード部（コンテンツ復号化出力手段）
３５　　ＥＣＭ－Ｋｃ解析部（経過時間情報第一暗号鍵取得手段）
３７　　ＥＣＭ－Ｋｗ解析部
３９　　Ｋｃ配布用ＥＣＭ解析部（利用制御情報第二暗号鍵取得手段）
４１　　再暗号化Ｋｃ配布用ＥＣＭ生成解析部（再暗号化手段）
４３　　Ｋｃ配布用ＥＭＭ解析部
４５　　再生時間カウンタ部（再生時間カウント手段）
４７　　視聴プレビュー判定部（視聴可能判定手段）
４９　　送出制御部
５１　　ＶｉｅｗＬｏｇ課金部（課金手段）

【書類名】　　図面

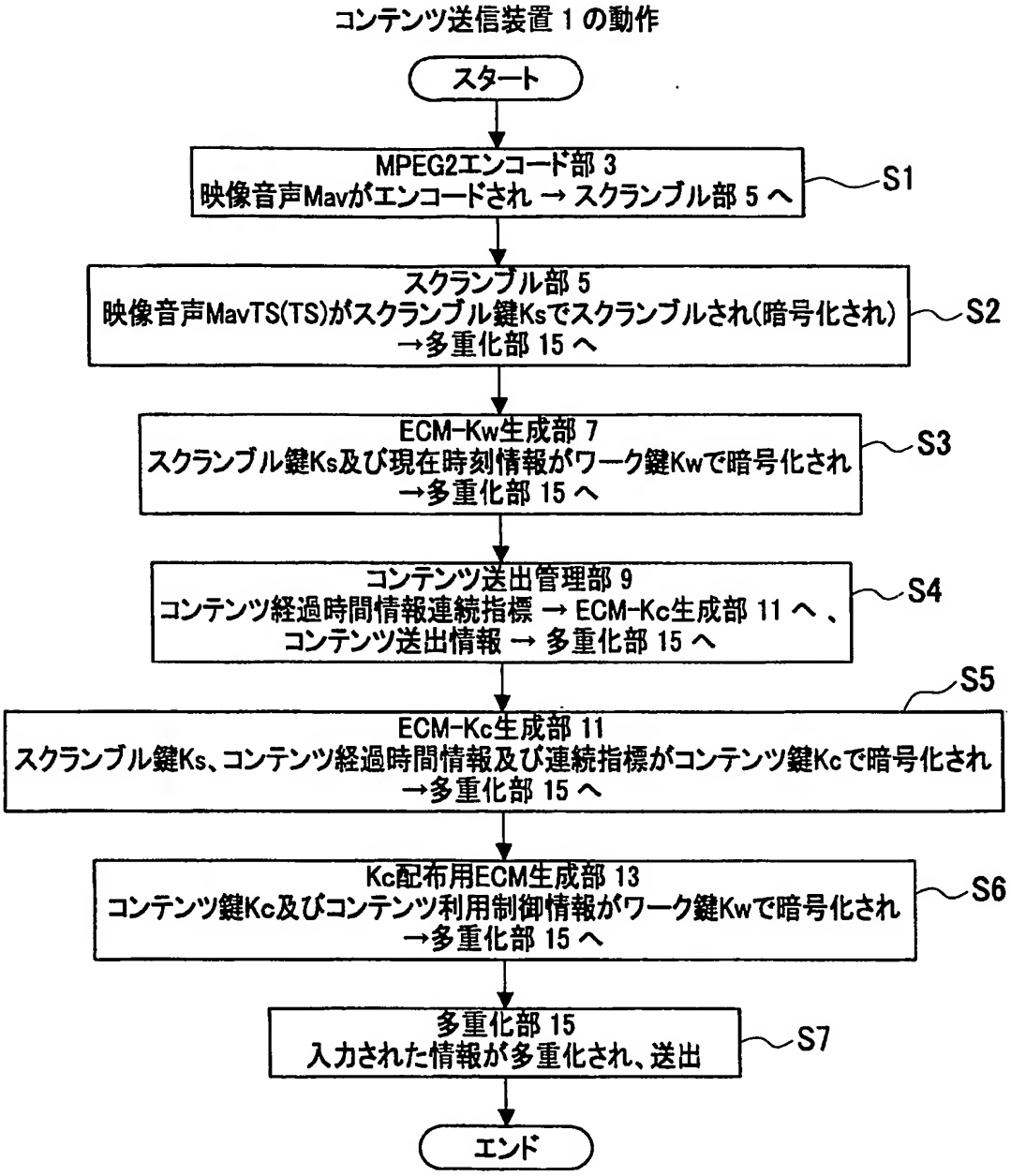
【図１】


1
15
送出
多重化部
E(Mav,Ks)
5
スクランブル部
暗号化
Ks
TS
3
MPEG2エンコード部
映像
音声Mav
E(ECM-Kw,Kw)
ECM-Kw
生成部
7
暗号化
ワーク鍵
Kw
E(ECM-Kc,Kc)
ECM-Kc
生成部
11
暗号化
コンテンツ鍵
Kc
コンテンツ送出情報
(EIT,SDTなど)
E(Kc配布用ECM,Kw)
Kc配布用
ECM生成部
13
暗号化
ワーク鍵
Kw
スクランブル鍵
現在時刻情報
コンテンツ
経過時間情報
連続指標
コンテンツ
送出管理部
9
現在時刻情報
コンテンツ利用制御情報
有効期限
プレビュー開始時刻・終了時刻
プレビュー再生許可時間
購入フラグ

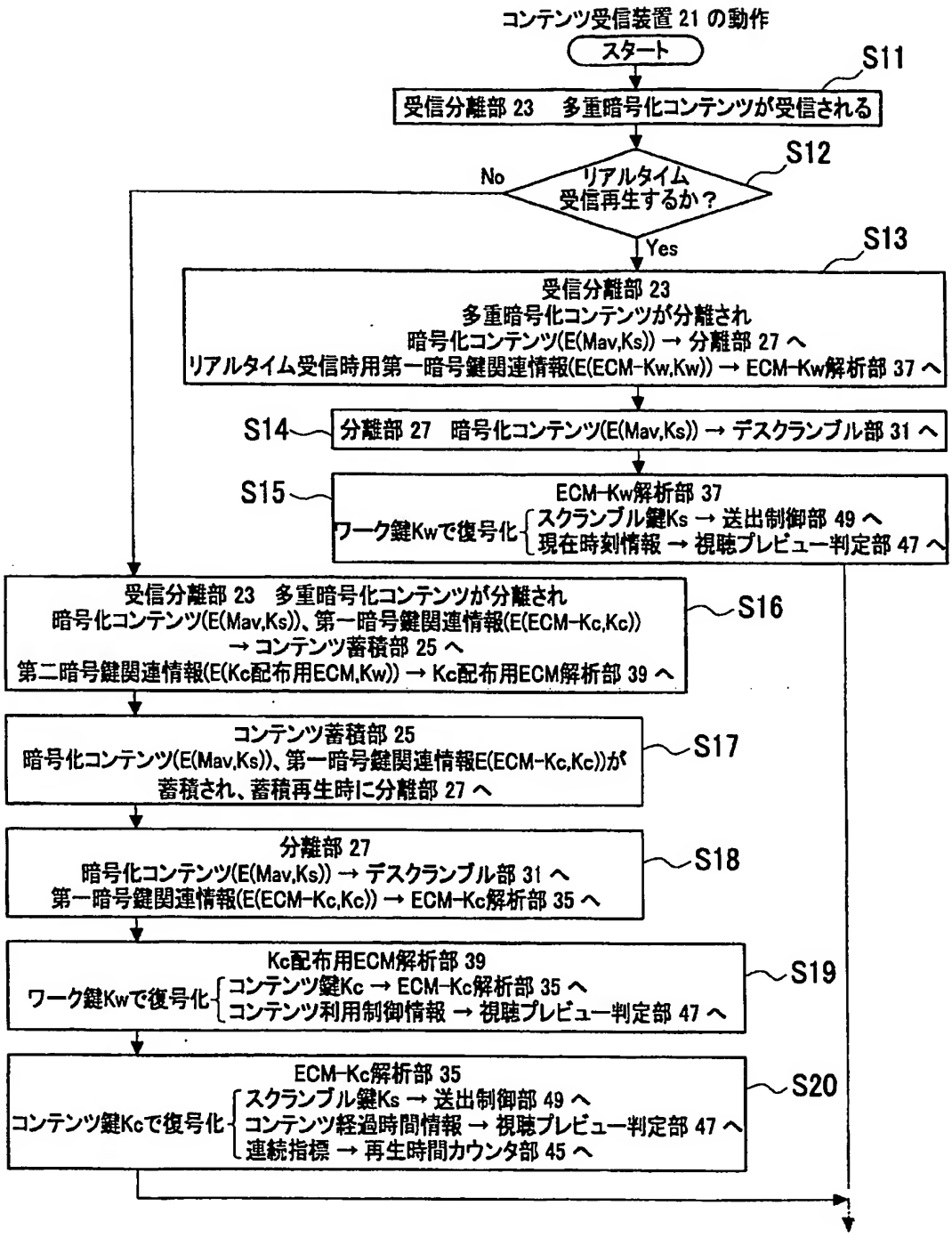
【図２】


21
Mav
23
27
33
MPEG2デコード部
TS
分離部
映像・音声
E(Mav,Ks)
デスクランブル部
E(ECM-Kc,Kc)
31
Ks
コンテンツ蓄積部
29
(蓄積再生時)
49
Ks
25
ECM-Kc解析部
送出制御部
35
コンテンツ経過時間情報
復号化
47
再暗号化Kc配布用ECM
Kc
コンテンツ鍵
視聴プレビュー判定部
Ks
連続指標
(リアルタイム受信再生時)
受信
受信分離部
E(ECM-Kw,Kw)
ECM-Kw解析部
再生時間カウンタ部
現在時刻情報
37
復号化
45
ワーク鍵
Kw
Kc
コンテンツ利用制御情報
E(Kc配布用ECM,Kw)
Kc配布用ECM解析部
復号化された Kc配布用ECM
39
復号化
ワーク鍵
Kw
再暗号化Kc配布用ECM生成解析部
(再復号化された)コンテンツ利用制御情報
41
再生時間購入フラグ
ViewLog課金部
暗号化/復号化
51
固有鍵
Kc
Kc配布用EMM
Kc配布用EMM解析部
43
復号化
共通鍵
セキュリティモジュール

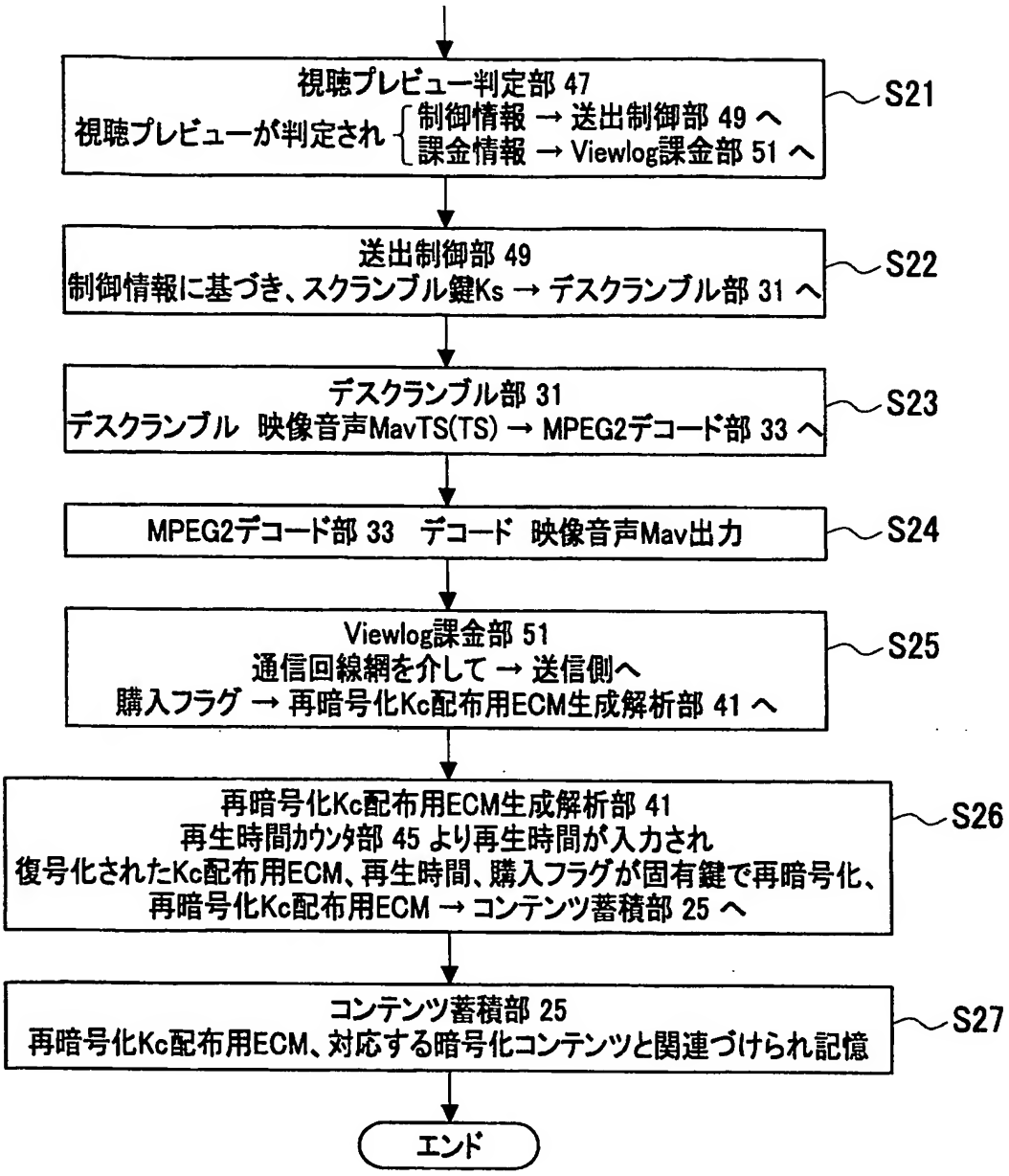
【図３】


コンテンツ送信装置１の動作
スタート
MPEG2エンコード部 3
映像音声Mavがエンコードされ → スクランブル部 5 へ
S1
スクランブル部 5
映像音声MavTS(TS)がスクランブル鍵Ksでスクランブルされ(暗号化され)
→多重化部 15 へ
S2
ECM-Kw生成部 7
スクランブル鍵Ks及び現在時刻情報がワーク鍵Kwで暗号化され
→多重化部 15 へ
S3
コンテンツ送出管理部 9
コンテンツ経過時間情報連続指標 → ECM-Kc生成部 11 へ 、
コンテンツ送出情報 → 多重化部 15 へ
S4
S5
ECM-Kc生成部 11
スクランブル鍵Ks、コンテンツ経過時間情報及び連続指標がコンテンツ鍵Kcで暗号化され
→多重化部 15 へ
Kc配布用ECM生成部 13
コンテンツ鍵Kc及びコンテンツ利用制御情報がワーク鍵Kwで暗号化され
→多重化部 15 へ
S6
多重化部 15
入力された情報が多重化され、送出
S7
エンド

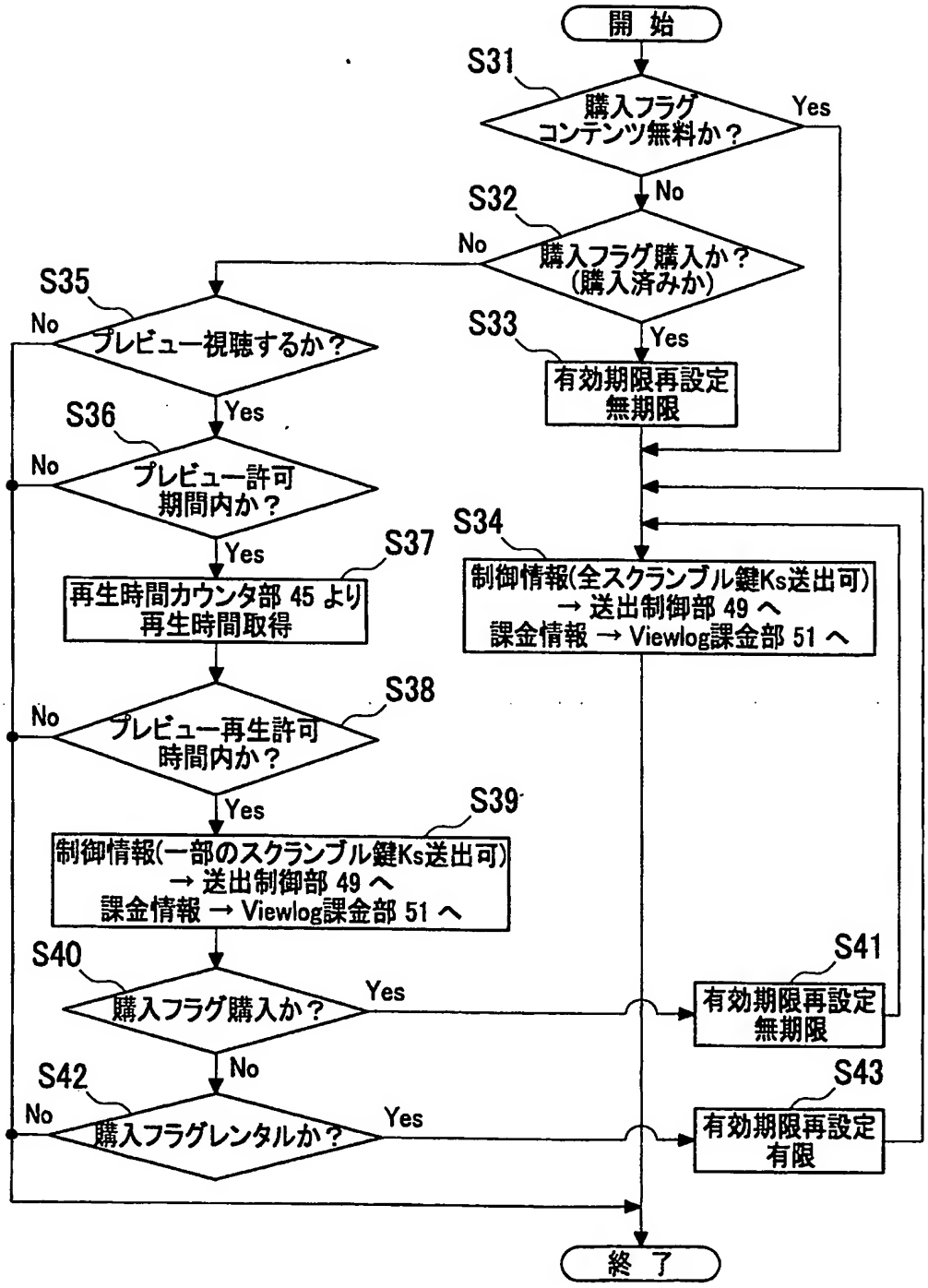
【図４】


コンテンツ受信装置 21 の動作
スタート
S11
受信分離部 23　多重暗号化コンテンツが受信される
S12
No
リアルタイム
受信再生するか？
Yes
S13
受信分離部 23
多重暗号化コンテンツが分離され
暗号化コンテンツ(E(Mav,Ks)) → 分離部 27 へ
リアルタイム受信時用第一暗号鍵関連情報(E(ECM-Kw,Kw)) → ECM-Kw解析部 37 へ
S14
分離部 27　暗号化コンテンツ(E(Mav,Ks)) → デスクランブル部 31 へ
S15
ECM-Kw解析部 37
ワーク鍵Kwで復号化
スクランブル鍵Ks → 送出制御部 49 へ
現在時刻情報 → 視聴プレビュー判定部 47 へ
受信分離部 23　多重暗号化コンテンツが分離され
暗号化コンテンツ(E(Mav,Ks))、第一暗号鍵関連情報(E(ECM-Kc,Kc))
→ コンテンツ蓄積部 25 へ
第二暗号鍵関連情報(E(Kc配布用ECM,Kw)) → Kc配布用ECM解析部 39 へ
S16
コンテンツ蓄積部 25
暗号化コンテンツ(E(Mav,Ks))、第一暗号鍵関連情報E(ECM-Kc,Kc))が
蓄積され、蓄積再生時に分離部 27 へ
S17
分離部 27
暗号化コンテンツ(E(Mav,Ks)) → デスクランブル部 31 へ
第一暗号鍵関連情報(E(ECM-Kc,Kc)) → ECM-Kc解析部 35 へ
S18
Kc配布用ECM解析部 39
ワーク鍵Kwで復号化
コンテンツ鍵Kc → ECM-Kc解析部 35 へ
コンテンツ利用制御情報 → 視聴プレビュー判定部 47 へ
S19
ECM-Kc解析部 35
コンテンツ鍵Kcで復号化
スクランブル鍵Ks → 送出制御部 49 へ
コンテンツ経過時間情報 → 視聴プレビュー判定部 47 へ
連続指標 → 再生時間カウンタ部 45 へ
S20

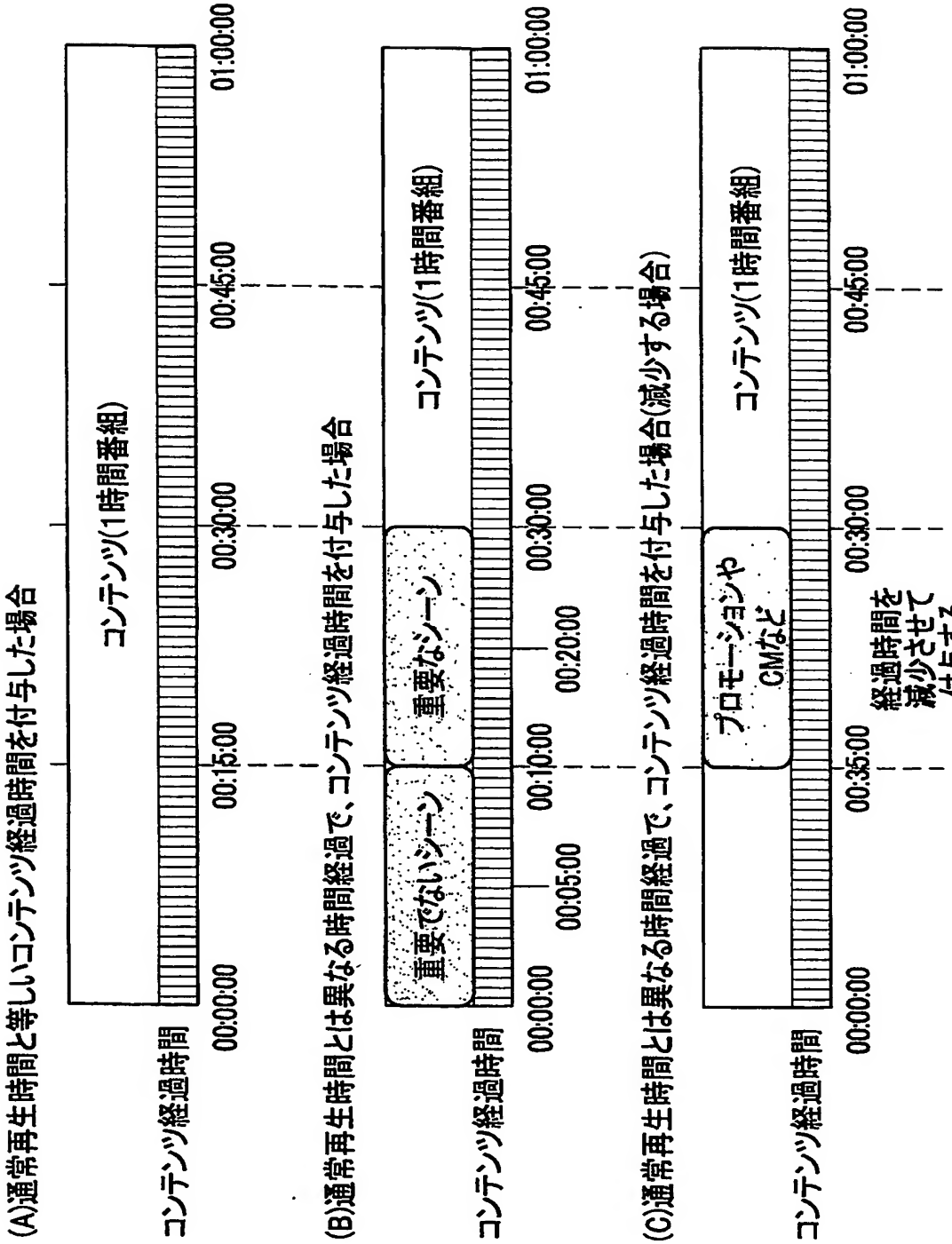
【図５】


視聴プレビュー判定部 47
視聴プレビューが判定され
制御情報 → 送出制御部 49 へ
課金情報 → Viewlog課金部 51 へ
S21
送出制御部 49
制御情報に基づき、スクランブル鍵Ks → デスクランブル部 31 へ
S22
デスクランブル部 31
デスクランブル 映像音声MavTS(TS) → MPEG2デコード部 33 へ
S23
MPEG2デコード部 33 デコード 映像音声Mav出力
S24
Viewlog課金部 51
通信回線網を介して → 送信側へ
購入フラグ → 再暗号化Kc配布用ECM生成解析部 41 へ
S25
再暗号化Kc配布用ECM生成解析部 41
再生時間カウンタ部 45 より再生時間が入力され
復号化されたKc配布用ECM、再生時間、購入フラグが固有鍵で再暗号化、
再暗号化Kc配布用ECM → コンテンツ蓄積部 25 へ
S26
コンテンツ蓄積部 25
再暗号化Kc配布用ECM、対応する暗号化コンテンツと関連づけられ記憶
S27
エンド

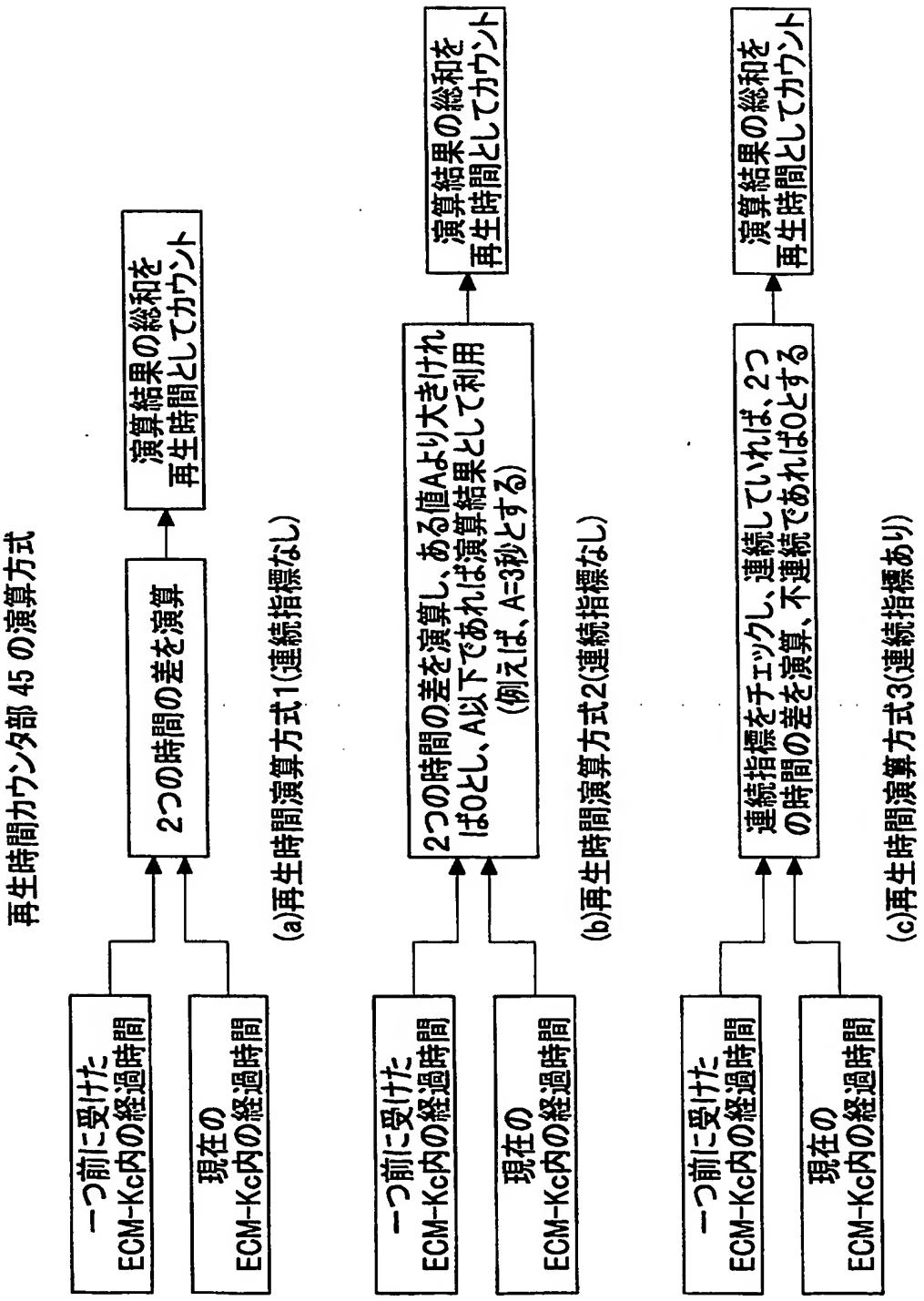
【図６】


開 始
S31
購入フラグ
コンテンツ無料か？
Yes
No
S32
No
購入フラグ購入か？
(購入済みか)
S35
No
プレビュー視聴するか？
S33
Yes
有効期限再設定
無期限
S36
Yes
No
プレビュー許可
期間内か？
S34
Yes
S37
制御情報(全スクランブル鍵Ks送出可)
→ 送出制御部 49 へ
課金情報 → Viewlog課金部 51 へ
再生時間カウンタ部 45 より
再生時間取得
S38
No
プレビュー再生許可
時間内か？
Yes
S39
制御情報(一部のスクランブル鍵Ks送出可)
→ 送出制御部 49 へ
課金情報 → Viewlog課金部 51 へ
S40
購入フラグ購入か？
Yes
S41
有効期限再設定
無期限
No
S42
No
購入フラグレンタルか？
Yes
S43
有効期限再設定
有限
終 了

【図７】


(A)通常再生時間と等しいコンテンツ経過時間を付与した場合
コンテンツ(1時間番組)
コンテンツ経過時間
00:00:00
00:15:00
00:30:00
00:45:00
01:00:00
(B)通常再生時間とは異なる時間経過で、コンテンツ経過時間を付与した場合
重要でないシーン
重要なシーン
コンテンツ(1時間番組)
コンテンツ経過時間
00:00:00
00:05:00
00:10:00
00:20:00
00:30:00
00:45:00
01:00:00
(C)通常再生時間とは異なる時間経過で、コンテンツ経過時間を付与した場合(減少する場合)
プロモーションやCMなど
コンテンツ(1時間番組)
コンテンツ経過時間
00:00:00
00:35:00
00:30:00
00:45:00
01:00:00
経過時間を減少させて付与する

【図８】


再生時間カウンタ部 45 の演算方式
一つ前に受けたECM-Kc内の経過時間
現在のECM-Kc内の経過時間
2つの時間の差を演算
演算結果の総和を再生時間としてカウント
(a)再生時間演算方式1(連続指標なし)
一つ前に受けたECM-Kc内の経過時間
現在のECM-Kc内の経過時間
2つの時間の差を演算し、ある値Aより大きければ0とし、A以下であれば演算結果として利用(例えば、A=3秒とする)
演算結果の総和を再生時間としてカウント
(b)再生時間演算方式2(連続指標なし)
一つ前に受けたECM-Kc内の経過時間
現在のECM-Kc内の経過時間
連続指標をチェックし、連続していれば、2つの時間の差を演算、不連続であれば0とする
演算結果の総和を再生時間としてカウント
(c)再生時間演算方式3(連続指標あり)

(a)

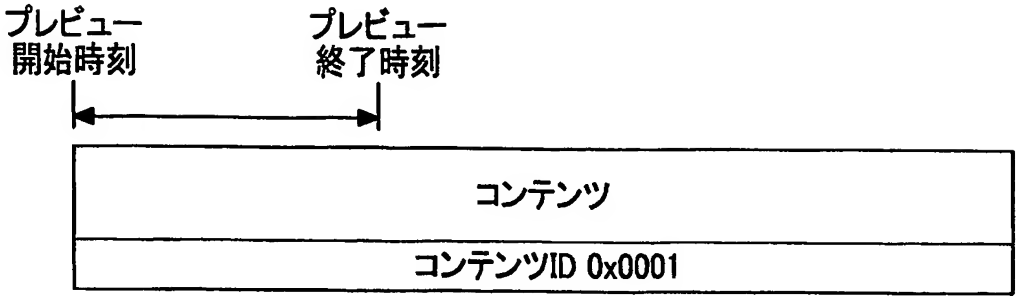
| 有効期限 | プレビュー開始時刻 | プレビュー終了時刻 | プレビュー再生許可時間 | 購入フラグ |
|---|---|---|---|---|
| 02/08/06 24:00:00 | 00:00:00 | 00:00:15 | 00:00:20 | PF |

(b)

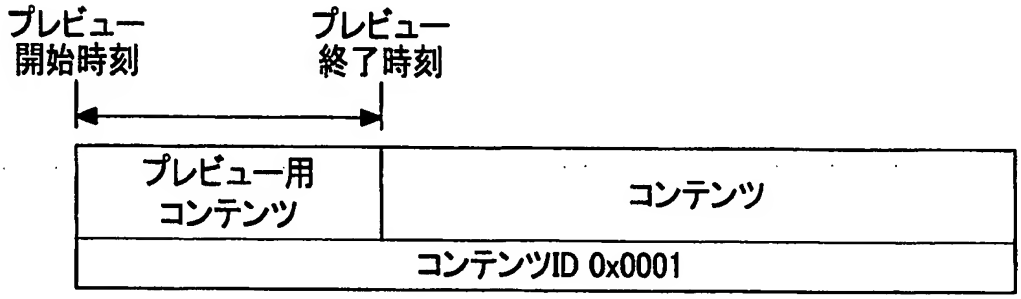
| コンテンツID | コンテンツ鍵Kc | 有効期限 | プレビュー開始時刻 | プレビュー終了時刻 | プレビュー再生許可時間 | 再生時間 | 購入フラグ |
|---|---|---|---|---|---|---|---|
| 0x00000001 | 0xAABBCCDD EEFFGGHH・・・ | 02/08/06 24:00:00 | 00:00:00 | 00:00:15 | 00:00:20 | PT | PF |
| 0x00000002 | | | | | | | |
| 0x00000003 | | | | | | | |
| 0x00000004 | | | | | | | |
| 0x00000005 | | | | | | | |
| 0x00000006 | | | | | | | |
| 0x00000007 | | | | | | | |

【図１０】

(a)


プレビュー
開始時刻
プレビュー
終了時刻
コンテンツ
コンテンツID 0x0001

(b)


プレビュー
開始時刻
プレビュー
終了時刻
プレビュー用
コンテンツ
コンテンツ
コンテンツID 0x0001

【書類名】　　要約書

【要約】

【課題】　蓄積再生時に、プレビューを視聴することができ、編集したプレビュー用コンテンツを取り扱うことができ、より細かくプレビュー制御できるコンテンツ送信方法、装置、プログラムおよびコンテンツ受信方法、装置、プログラムを提供する。

【解決手段】　受信側でコンテンツを蓄積後、当該コンテンツの特定部分を取り出して同コンテンツの特定部分以外の部分に対して異なる視聴形態で視聴可能にするコンテンツ送信装置１であって、コンテンツをスクランブル鍵Ｋｓで暗号化するスクランブル部５と、スクランブル鍵Ｋｓおよびコンテンツ経過時間情報をコンテンツ鍵Ｋｃで暗号化するＥＣＭ－Ｋｃ生成部１１と、コンテンツ鍵Ｋｃおよびコンテンツ利用制御情報をワーク鍵Ｋｗで暗号化するＫｃ配布用ＥＣＭ生成部１３と、多重化して送出する多重化部１５と、を備えた。

【選択図】　　図１

特願２００２－２４８８１２

出　願　人　履　歴　情　報

識別番号　　［０００００４３５２］

１．変更年月日　　１９９０年　８月　８日
［変更理由］　　新規登録
住　所　　東京都渋谷区神南２丁目２番１号
氏　名　　日本放送協会